William Anderson Eloi de Carvalho

VIGILÂNCIA DAS FORÇAS DE SEGURANÇA ATRAVÉS DE CÂMERAS DE RECONHECIMENTO FACIAL E O CONFLITO COM O DIREITO À PRIVACIDADE – BRASIL E PORTUGAL

Dissertação com vista à obtenção do grau de
Mestre em Direito e Segurança

Orientador:
Doutor Luciano Loiola da Silva

Setembro de 2019

VIGILÂNCIA DAS FORÇAS DE SEGURANÇA ATRAVÉS DE CÂMERAS DE RECONHECIMENTO FACIAL E O CONFLITO COM O DIREITO À PRIVACIDADE – BRASIL E PORTUGAL

DISSERTAÇÃO DE MESTRADO EM DIREITO E SEGURANÇA DA FACULDADE DE DIREITO DA UNIVERSIDADE NOVA DE LISBOA, COM A FINALIDADE DE OBTENÇÃO DO GRAU DE MESTRE EM DIREITO E SEGURANÇA

AUTOR: WILLIAM ANDERSON ELOI DE CARVALHO

ORIENTADOR: DOUTOR LUCIANO LOIOLA DA SILVA

Setembro de 2019

VIGILÂNCIA DAS FORÇAS DE SEGURANÇA ATRAVÉS DE CÂMERAS DE RECONHECIMENTO FACIAL E O CONFLITO COM O DIREITO À PRIVACIDADE – BRASIL E PORTUGAL

William Anderson Eloi de Carvalho

Setembro 2019

Declaração antiplágio

Declara-se que é original o trabalho agora apresentado em forma de dissertação para obtenção do grau de Mestre em Direito e Segurança, sob o título: VIGILÂNCIA DAS FORÇAS DE SEGURANÇA ATRAVÉS DE CÂMERAS DE RECONHECIMENTO FACIAL E O CONFLITO COM O DIREITO À PRIVACIDADE – BRASIL E PORTUGAL. Toda utilização de contribuições ou textos alheios está devidamente referenciada. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Agradecimentos

Gostaria de agradecer:

A Deus, pois sem Ele eu nada sou e nada poderia fazer. À Ele toda honra, toda glória e todo louvor.

À minha amada esposa e meu porto seguro, Larissa Figueiredo Belo de Carvalho, que sempre esteve ao meu lado durante essa jornada. Sem ela eu não chegaria aqui. Ela me incentivou a dar o primeiro passo dessa jornada, sem nem eu mesmo acreditar que seria possível. Nas vezes que pensei em desistir, ela me trouxe palavras de incentivo e ânimo, fazendo com que eu mantivesse o foco.

Aos meus pais, Miguel e Ana Maria, que me ensinaram todos os valores morais que formam o meu caráter. Sou quem sou graças a vocês. Vocês são parte de todas as minhas conquistas.

Aos meus irmãos, Miguel Jr. e Juliana, que são meus amigos desde que nasci e sempre me apoiam nas minhas lutas.

Ao meu orientador, Doutor Luciano Loiola da Silva, Major da Polícia Militar do Distrito Federal, pela paciência, orientação, apontamentos, conversas amigáveis e incentivo, que foram essenciais para concluir essa jornada.

Ao meu companheiro, Renzo Medina Dallago, Capitão da Polícia Militar do Distrito Federal, que caminhou junto comigo nessa trajetória e contribuiu significativamente para a conclusão deste projeto.

Aos amigos que fiz no período que morei em Portugal em 2017/18, principalmente os integrantes da Guarda Nacional Republicana e das Forças Armadas portuguesas, que me proporcionaram momentos únicos na vida.

À Polícia Militar do Distrito Federal, que me possibilitou essa experiência profissional extraordinária, quando abriu o processo seletivo para frequentar o Curso de Promoção a Oficial Superior, da Guarda Nacional República.

Lista de abreviaturas, siglas e acrónimos

CFTV	Circuito Fechado de Televisão
CCTV	Closed Circuit Television
ONU	Organização das Nações Unidas
RGPD	Regulamento Geral sobre a Proteção de Dados
UE	União Europeia
LGPD	Lei Geral de Proteção de Dados
DUDH	Declaração Universal dos Direitos Humanos
FBSP	Fórum Brasileiro de Segurança Pública
IPEA	Instituto de Pesquisa Econômica Aplicada
USP	Universidade de São Paulo
PIB	Produto Interno Bruto
OMS	Organização Mundial da Saúde
UNODC	United Nations Office on Drugs and Crime
EUA	Estados Unidos da América
GPI	Global Peace Index
IEP	Institute for Economics & Peace
IACP	International Association of Chiefs of Police
ATM	Automated Teller Machine
DCC	Distritos Comerciais Centrais
DMV	Departamento de Veículos Motorizados
ARJIS	Automated Regional Justice Information System
AFR	Automated Facial Recognition
UEFA	Union of European Football Associations
PSL	Partido Social Liberal
CRFB/88	Constituição da República Federativa do Brasil de 1988
CRP	Constituição da República Portuguesa
PIDE	Polícia Internacional e de Defesa do Estado
DGS	Direção-geral de Segurança
CNPDI	Comissão Nacional de Proteção de Dados Pessoais Informatizados
CNPD	Comissão Nacional de Proteção de Dados
GDPR	General Data Protection Regulation

LED	Law Enforcement Data Protection Directive
PNR	Passenger Name Record
ANPD	Autoridade Nacional de Proteção de Dados
MPDFT	Ministério Público do Distrito Federal e Territórios
IDP	Instituto Brasiliense de Direito Público
STF	Supremo Tribunal Federal

Declaração de conformidade

O corpo da dissertação, incluindo espaços e notas, ocupa um total de 273.763 caracteres.

Resumo

Esta dissertação tem como objetivo analisar o conflito entre o direito à privacidade e a utilização de câmeras de reconhecimento facial pelas forças de segurança, no Brasil e em Portugal. O objetivo é responder a seguinte pergunta: O direito à privacidade impede o emprego da tecnologia de reconhecimento facial na segurança pública? Primeiramente, importa destacar o contexto de segurança pública dos dois países, onde o Brasil possui índices de homicídio semelhantes aos de países em guerra, enquanto Portugal é considerado um dos países mais seguros do mundo. Esse abismo entre os dois países faz com que eles tenham realidades muito distintas em relação à segurança pública e o emprego de novas tecnologias. Estudos sobre Circuito Fechado de Televisão (CFTV) e sobre a tecnologia de reconhecimento facial, demonstram que ambos são eficazes no combate à criminalidade, desde que utilizados de forma conjunta com outros métodos e com a interferência do ser humano no processo. Mas para saber se essa tecnologia pode ser utilizada, foi preciso analisar a legislação, do Brasil e de Portugal, onde se observou que os dois países possuem leis específicas que abordam esse assunto. Diante da análise do Regulamento Geral sobre a Proteção de Dados (RGPD), de 2016, e da Diretiva (UE) 2016/680, ambos da União Europeia, bem como, da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/18, alterada pela Lei nº 13.853, de 8 de julho de 2019, do Brasil, chega-se à conclusão que, apesar do conflito de direitos fundamentais apresentado pelo caso concreto, essa legislação harmoniza a coexistência desses direitos, permitindo a proteção dos direitos e garantias fundamentais, ao mesmo tempo que cria um cenário favorável ao progresso tecnológico e à livre circulação dos dados pessoais. Assim, a resposta à pergunta inicial é que, para Brasil e Portugal, o direito à privacidade não impede o emprego da tecnologia de reconhecimento facial na segurança pública.

Palavras-chaves

Reconhecimento facial. Direito à privacidade. CFTV. Segurança pública. Brasil. Portugal. Conflito de direitos.

Abstract

This dissertation aims to analyze the conflict between the right to privacy and the use of face recognition cameras by security forces in Brazil and Portugal. The goal is to answer the following question: Does the right to privacy prevent the use of facial recognition technology in public safety? Before the answer is reached, the theme is contextualized, where the reality of both countries is verified, regarding public safety, and the gulf that separates Brazil from Portugal, where the former has homicide rates similar to those of countries at war, and the second is considered one of the safest countries in the world. Next, a study is done on Closed Circuit Television (CCTV) and facial recognition technology, showing how the system works and presenting data that prove its effectiveness. Then, legislation is analyzed from Brazil and Portugal to determine whether it is possible to employ CCTV systems with face recognition technology by the security forces, or whether this limits or prevents the exercise of rights and guarantees of citizens, focusing mainly on the right to privacy and the protection of personal data. Finally, the last chapter concludes the discussion, concluding that it is a conflict of fundamental rights, where current legislation harmonizes the coexistence of these rights, allowing the protection of fundamental rights and guarantees, while creating a scenario favorable to technological progress and the free movement of personal data. Thus, the answer to the original question is that, for Brazil and Portugal, the right to privacy does not prevent the use of facial recognition technology in public safety.

Keywords

Facial recognition. Right to privacy. CCTV. Public safety. Brazil. Portugal. Conflict of rights.

SUMÁRIO

Índice de Figuras

INTRODUÇÃO

A presente dissertação de mestrado, desenvolvida no âmbito do Mestrado em Direito e Segurança, da Faculdade de Direito da Universidade Nova de Lisboa, aprofunda a discussão sobre o impacto da tecnologia de reconhecimento facial nas liberdades e garantias individuais das pessoas, principalmente no direito à privacidade, analisando e comparando as legislações de Brasil e Portugal, com o seguinte tema: Vigilância das forças de segurança através de câmeras de reconhecimento facial e o conflito com o direito à privacidade – Brasil e Portugal.

A criminalidade organizada e a escassez de meios, onde o Estado tem o dever de fazer mais com menos, impõem uma segurança pública cada vez mais preparada e avançada tecnologicamente, onde não é mais suficiente o policial na rua e a viatura patrulhando, e sim a utilização de ferramentas tecnológicas para otimizar o policiamento e trazer mais segurança ao cidadão.

Atualmente, os avanços tecnológicos trouxeram ao mercado da segurança pública as câmeras de reconhecimento facial, que através da leitura de pontos nodais da face – como distância entre os olhos, largura do nariz, comprimento da linha da mandíbula, etc. – são capazes de detectar rostos em uma multidão e comparar, em poucos segundos, com uma imensa base de dados.

Casos de sucesso como o da polícia de Faxian/China, que prendeu 80 suspeitos em menos de um ano, com a ajuda da tecnologia de reconhecimento facial; da polícia indiana, que em apenas quatro dias do lançamento do sistema, em Nova Delhi, reconheceu 2.930 crianças que estavam desaparecidas; e da polícia militar do Rio de Janeiro/Brasil, que nos primeiros dez dias de março, o sistema ajudou na captura de oito pessoas que estavam com mandado de prisão ou apreensão em aberto, além da recuperação de três veículos roubados; aliado com estudos que comprovam a efetividade de sistemas de Circuito Fechado de Televisão (CFTV), trazem um cenário animador para as polícias de todo o mundo.

Mas o Estado pode controlar tamanho poder de informação sem incorrer em violações aos direitos e garantias individuais dos cidadãos? O direito à privacidade impede o emprego da tecnologia de reconhecimento facial na segurança pública? Essas são questões a serem respondidas por esse trabalho. Nesse cenário, o direito à privacidade seria o mais ameaçado.

O primeiro estudo jurídico sobre o direito à privacidade foi o artigo *The Right to Privacy* (O Direito à Privacidade), escrito por Samuel D. Warren e Louis Brandeis, e publicado na *Havard Law Review*, em 1890, que consagrou esse direito como "*right to be let alone*"(o direito de ser deixado sozinho).

Desde então, várias documentos internacionais consagraram o direito à privacidade, como a Declaração Universal dos Direitos do Homem, de 1948; a Convenção Europeia de Salvaguarda dos Direitos do Homem e das Liberdades Fundamentais, de 1950; o Pacto Internacional relativo aos direitos civis e políticos, Organização das Nações Unidas (ONU), em 1966; a Convenção Americana sobre os Direitos do Homem, São José da Costa Rica/1969; dentre outros.

O direito à privacidade é um direito fundamental, tanto no Brasil, como em Portugal, essencial para o desenvolvimento da personalidade individual de cada pessoa. Ele compõe os direitos de personalidade e são tidos como direitos absolutos, pois se estabelecem como uma obrigação passiva universal e impõem o dever de respeito por todos. Portanto, é imprescindível que o Estado defenda o direito à privacidade.

Nesse sentido, surge o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, que entrou em vigor em 2016 e se tornou aplicável desde 25 de maio de 2018. O RGPD veio justamente para proteger os direitos e garantias fundamentais dos cidadãos, com objetivo de diminuir os riscos da coleta e uso, compartilhamento, armazenamento, entre outros, dos dados pessoais.

Juntamente com o RGPD, foi publicada a Diretiva (UE) 2016/680, que aborda, especificamente, o tratamento de dados pessoais realizado por autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, com a finalidade de proteger os direitos e das liberdades fundamentais das pessoas, sem que isso limite intercâmbio de dados pessoais entre autoridades competentes na União.

O RGPD causou um “efeito cascata” na legislação de outros países e nas empresas, que tiveram que se adequar ao RGPD para manter relações comerciais com a União Europeia.

Com isso, o Brasil criou a Lei Geral de Proteção de Dados (LGPD), através da Lei nº 13.709/18, alterada pela Lei nº 13.853, de 8 de julho de 2019. Apesar de ainda recente, essa lei veio para resguardar os direitos fundamentais da liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, no que se refere ao tratamento de dados pessoais.

Através do estudo dessas legislações e do direito à privacidade, bem como do conflito de direitos fundamentais e de princípios, essa dissertação visa alcançar uma resposta para os quesitos expostos acima.

1. CONTEXTUALIZAÇÃO DO TEMA

1.1. Conceito de Estado

O conceito de Estado é uma construção histórica de vários autores, de forma que esse conceito foi evoluindo ao longo da história até chegar na ideia que se tem hoje.

Para Thomas Hobbes (2003), as paixões e desejos do ser humano não são, por si só, um pecado. Nem sequer as ações que procedem dessas paixões, até que exista uma lei que as proíba. Segundo Hobbes, nenhuma lei pode ser feita sem que antes se determine qual pessoa irá fazê-la. Ou seja, todos os desejos dos homens são lícitos até que exista uma lei que os torne proibidos. Assim, para que os seres humanos tenham limites para uma convivência pacífica, deve existir lei, e com isso, alguém incumbido de editá-la.

O Estado seria essa "pessoa", uma organização da sociedade dona da liberdade e da propriedade de todos. Para que não houvesse um total descontrole social, as pessoas deveriam aprovar os atos e decisões do Estado, como se fossem feitas elas próprias.

Além disso, para Thomas Hobbes (2003, p. 143), "os pactos sem a espada não passam de palavras, sem força para dar qualquer segurança a ninguém". Logo, se não houver um poder suficientemente grande para a segurança do povo, nesse caso um Estado soberano e forte, cada um irá confiar apenas em sua própria força e capacidade, como meio de proteção contra os outros.

Nesse sentido, Hobbes afirma que é necessário intitular um homem ou uma assembleia de homens, como representante do povo, de forma que todos submetam seus anseios à vontade do representante, e suas decisões à sua convicção. Seria isso mais do que um simples consentimento, seria uma verdadeira unidade de todos, como se cada indivíduo realizasse um pacto com todos os outros, como se cada homem dissesse ao outro: Entrego meu direito de me governar a este representante e autorizo todas as suas ações. "Feito isso a multidão assina unida numa só pessoa que se chama Estado, em latim *civitas*." (Hobbes, 2003, p. 147).

O Estado é criado a partir de uma espécie de contrato entre as pessoas, as quais atribuem a força e poder do povo a um homem ou assembleia de homens. Com isso, o Estado tem poder suficiente para assegurar a paz e a defesa de todos.

Para John Locke (1998) o principal motivo para que homens se reúnam em sociedade e deixem seu estado de natureza, é que nessa sociedade existe autoridade, um poder onde é possível conseguir amparo mediante apelo, nesse caso, o estado de guerra é extinto e as

contradições por aquele poder. Assim, os homens se reúnem em sociedade e criam suas leis para evitar a guerra entre eles.

Através dessas leis, o Estado tem o poder de fazer cessar conflitos, com o objetivo maior de manter a paz e a ordem social. O objetivo maior dos homens aderirem a uma sociedade é o gozo da sociedade em paz e segurança, onde a grande ferramenta para esse fim são as normas estabelecidas nessa sociedade (Locke, 1998). Ou seja, as leis são determinadas para que os homens possam ter segurança e paz social, sendo necessária a criação da sociedade para este fim.

Para Jean-Jacques Rousseau (1999), o Estado era um conjunto de membros associados para um bem comum, onde cada homem, ao se dar a todos, não se dá a ninguém, de forma que cada um ganha o correspondente a tudo que se perde, e mais força para conservar o que se tem.

Quanto aos termos comumente associados ao Estado, a pessoa pública, formada pela união de todos os particulares, antigamente se dava o nome de cidade, que passou a se chamar república ou corpo político, que é chamado por seus membros de Estado quando passivo, soberano quando ativo, e potência quando comparado a seus semelhantes. Referente aos associados, estes recebem o nome de povo, coletivamente, e cidadãos, em particular, enquanto partícipes da autoridade soberana, e ainda, súditos, enquanto submetidos às leis do Estado (Rousseau, 1999).

Assim, esse Estado, para Rousseau (1999), era formado pelo corpo político e pelo corpo social, onde todos trabalhavam para os outros, e consequentemente para si. Onde a vontade geral reinava sobre a vontade individual, e esse tratado social tem a finalidade de preservar os contratantes.

Charles Montesquieu (2000) menciona a república democrática como o resultado do povo deter o poder soberano em uma república, ou seja, uma democracia. Na democracia, o povo exerce a função de monarca, sob certos aspectos, e de súdito sob outros. Contudo, somente pode exercer essa função de monarca através de seus sufrágios, que seria a expressão de suas vontades. Portanto, as leis que estabelecem o direito de sufrágio são fundamentais nesse governo.

Para Max Weber (2015) o Estado soberano moderno se define pelo monopólio do uso da força legítima, ou monopólio da violência legítima. Isso significa que a coerção é função exclusiva de certos agentes do Estado, e jamais de um agente da sociedade. Dessa forma, o Estado se torna responsável pela organização e pelo controle social.

Por fim, percebe-se que dentre todas essas teorias pontuadas existe um tópico em comum, um ponto de equilíbrio entre todas elas, um objetivo comum ao Estado referenciado por todos os autores: a segurança.

Essa segurança foi referenciada acima de diversas formas: para Hobbes, o "Estado tem poder suficiente para assegurar a paz e a defesa de todos"; para Locke, "o Estado tem o poder de fazer cessar conflitos, com o objetivo maior de manter a paz e a ordem social", sendo que "o objetivo maior dos homens aderirem a uma sociedade é o gozo da sociedade em paz e segurança"; para Rousseau, o "tratado social tem a finalidade de preservar os contratantes"; e para Weber, através do monopólio do uso da força legítima, "o Estado se torna responsável pela organização e pelo controle social".

Essas afirmações exprimem a necessidade de o Estado garantir a segurança do seu povo, segurança nas mais diversas formas de interpretação, como segurança física, de propriedade, jurídica, ordem pública e etc.

Assim, conclui-se que a principal razão da própria existência do Estado é que este possa garantir a segurança do seu povo em um determinado território, sendo esse o principal fator para o homem sair de seu estado de natureza para evoluir para uma organização social complexa como o Estado moderno.

1.2. Brasil, um dos países mais violentos do mundo

A Segurança Pública é um direito de todos os cidadãos. Este direito é referenciado nos Tratados e Convenções Internacionais que serão esmiuçados em capítulos posteriores. Mas cabe salientar aqui que Tratados como a Declaração Universal dos Direitos Humanos (DUDH); a Declaração Americana do Direitos e Deveres do Homem, de 1948; a Convenção Europeia dos Direitos do Homem, de 1953; a Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica), de 1969; entre outros; citam a segurança como um direito fundamental. O conceito de Segurança Pública nesses documentos é entendido como um direito humano que permite aos cidadãos o exercício dos demais direito previstos no ordenamento jurídico, em especial, proteção à vida, liberdade, reunião e propriedade (Minuscoli e Almeida, 2016).

No Brasil, esse é um tema relatado diariamente na imprensa e é uma aflição constante do cidadão, pois 38% dos brasileiros elegeram a segurança pública como sua maior preocupação (Confederação Nacional da Indústria, 2018). A sensação de insegurança, somada ao medo, está presente na vida de grande parte da sociedade civil brasileira,

principalmente nos grandes centros urbanos. Assim como o acesso à saúde, à educação e à moradia, a garantia de ir e vir com segurança é um direito fundamental previsto pela Constituição Federal de 1988, sendo dever do Estado assegurá-lo.

O Brasil contabilizou 63.880 mortes violentas ao longo de 2017. O número, que significa média de 175 mortes por dia (ou ainda 7,2 por hora), representa o novo recorde da violência no País, conforme o Anuário Brasileiro de Segurança Pública 2018, divulgado pelo Fórum Brasileiro de Segurança Pública (FBSP, 2018).

Segundo o estudo, este é o maior número de assassinatos registrados no Brasil desde o início dos registros pelo FBSP em 2013, e ainda, representa um aumento de 2,9% no total em relação ao ano anterior.

Os dados de homicídio são considerados um dos aspectos mais consistentes e confiáveis para se comparar a violência social e é, portanto, essencial para fazer comparações de paz entre os países. Outros tipos de crimes violentos são difíceis de comparar devido às variações em sistemas de coleta, classificação, leis e relatórios procedimentos entre diferentes países e municípios (Institute for Economics & Peace, 2018).

Em 2016, o Brasil já havia ultrapassado a taxa de 30 assassinatos para cada 100 mil habitantes, segundo o Atlas da Violência 2018, relatório elaborado pelo Instituto de Pesquisa Econômica Aplicada (IPEA) e pelo FBSP com base em dados do Ministério da Saúde. Com 62.517 homicídios, a taxa chegou a 30,3 assassinatos para cada 100 mil habitantes.

Ainda segundo o Atlas da Violência, entre 2006 e 2016, 553 mil pessoas perderam a vida vítimas de violência no Brasil. Esses números são maiores que os de mortos da Guerra Civil da Síria (Jornal da USP, 2018).

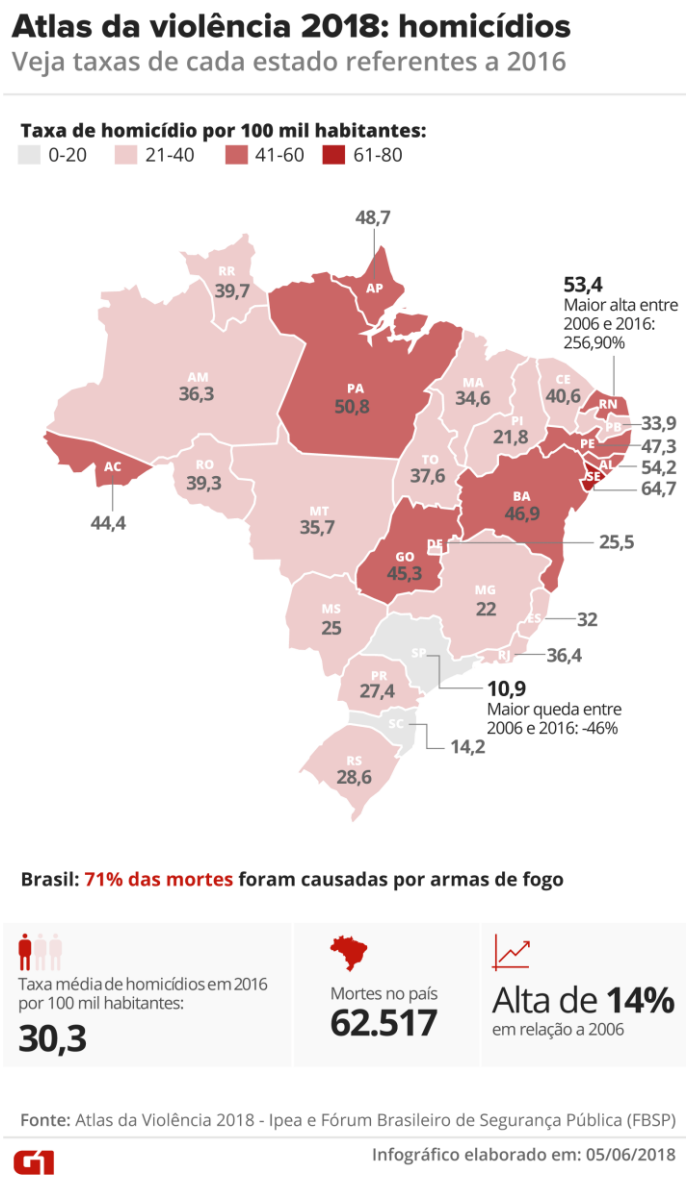

Figura 1: Taxa de homicídios de cada estado do Brasil referentes a 2016 (G1-Globo, 2018)

A Secretaria Especial de Assuntos Estratégicos da Presidência da República publicou, em junho de 2018, um Relatório de Conjuntura com o título de "Custos Econômicos da Criminalidade no Brasil", onde desenvolve uma metodologia para estimar os custos econômicos da criminalidade no Brasil para o período de 1996 a 2015 (Secretaria-Geral da Presidência do Brasil, 2018).

Dentre outras conclusões, o relatório aponta que o Brasil está entre os 10% de países com maiores taxas de homicídio do mundo. Apesar de ter uma população equivalente a 3% da população mundial, o país concentra cerca de 14% dos homicídios do mundo. As taxas de homicídio brasileiras são semelhantes às de Ruanda, República Dominicana, África do Sul e República Democrática do Congo.

A distribuição regional da violência no Brasil é significativamente desigual (ver Figura 2). Algumas microrregiões têm taxas de homicídio iguais ou menores que 10 por 100 mil habitantes, taxas comparáveis a países como Argentina, Uruguai, Equador ou Estados Unidos. Dentre estas, destaca-se a microrregião de São Paulo, que tem a maior população.

Por outro lado, algumas capitais no Norte-Nordeste, como Belém, Salvador, Fortaleza São Luís, além da microrregião do Entorno do Distrito Federal, têm taxas de 50 por 100 mil habitantes, o que as colocaria em níveis de alguns dos países mais violentos do mundo, como Jamaica, Venezuela e Honduras.

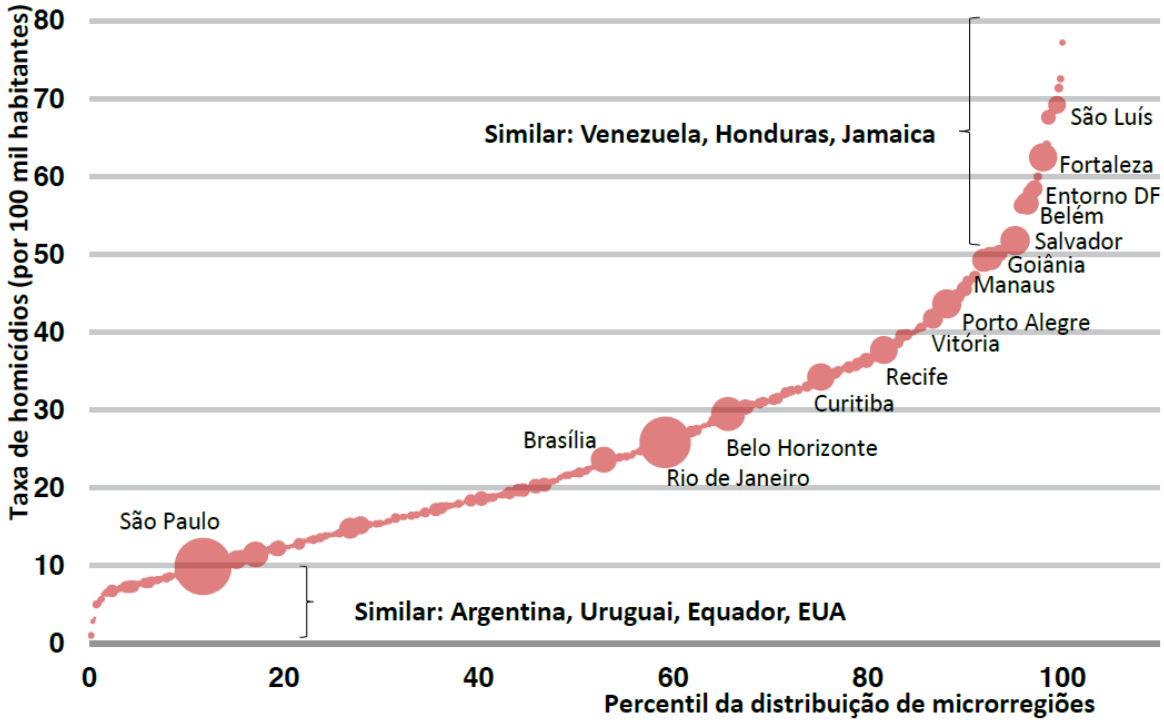

Figura 2: Brasil: Taxa de Homicídios por Microrregião, 2015 (Homicídios por 100 mil habitantes, bolhas proporcionais à população da microrregião) (Secretaria-Geral da Presidência do Brasil, 2018)

Referente ao propósito de estimar os custos econômicos da criminalidade, o relatório conclui que a perda cumulativa de capacidade produtiva decorrente de homicídios, entre 1996 e 2015, superou os 450 bilhões de reais, levando-se em conta que para cada homicídio de jovens de 13 a 25 anos, o valor calculado da perda da capacidade produtiva é de cerca de 550 mil reais.

Somente em 2015, a criminalidade custou R$ 285 bilhões ao Brasil, mas que o dobro dos 113 bilhões de 1996. Em 2015, os componentes, em ordem de relevância eram: segurança pública (1,35% do Produto Interno Bruto – PIB); segurança privada (0,94% do PIB); seguros e perdas materiais (0,8% do PIB); custos judiciais (0,58% do PIB); perda de capacidade produtiva (0,40% do PIB); encarceramento (0,26% do PIB); e custos dos

serviços médicos e terapêuticos (0,05% do PIB), alcançando um total de 4,38% da renda nacional.

De acordo com o *World Statistics* 2018, relatório publicado pela Organização Mundial da Saúde (OMS), o Brasil tem a sétima maior taxa de homicídio da região das Américas e a nona maior taxa do mundo, com um indicador de 31,3 mortes para cada 100 mil habitantes. Os maiores índices do mundo estão nas Américas, e pertencem à Honduras, com uma taxa de 55,5 mortes para cada 100 mil habitantes, Venezuela (49,2), que passou para a segunda posição antes ocupada por El Salvador (46), atualmente em terceiro lugar (World Health Organization, 2018).

Os dados da UNODC (United Nations Office on Drugs and Crime, 2018) demonstram que o Brasil é o país com o maior número de homicídios intencionais em números absolutos, superando país com populações muito maiores como a China e a Índia.

Nesse aspecto, a Revista Superinteressante publicou um artigo interessante com o nome "O Brasil tem mais assassinatos do que todos estes países somados", onde compara a quantidade de assassinatos no Brasil com a de outros países (Deursen, 2018).

Segundo a reportagem, o Brasil tem mais assassinatos do que a soma de todos os países destacados no mapa:

Figura 3: O Brasil tem mais assassinatos do que todos estes países somados (Deursen, 2018)

Ou seja, com 59 mil assassinatos em 2015, o Brasil teve mais homicídios que a soma de todos os seguintes países: Estados Unidos da América (EUA), Canadá, Marrocos, Argélia, Tunísia, Líbia, Egito, China, Mongólia, Malásia, Indonésia, Austrália, Nova Zelândia, Coreia do Sul, Coreia do Norte, Japão, Portugal, Espanha, Reino Unido, Irlanda, França, Bélgica, Holanda, Luxemburgo, Alemanha, Itália, Suíça, Dinamarca, Noruega, Suécia, Finlândia, Estônia, Letônia, Lituânia, Polônia, República Tcheca, Eslováquia, Áustria, Hungria, Belarus, Ucrânia, Romênia, Moldávia, Bulgária, Eslovênia, Croácia, Bósnia-Herzegóvina, Sérvia, Montenegro, Albânia, Grécia e Macedônia.

Alguém poderia dizer que nessa lista existem países que estão aí somente para aumentar o número de países, uma vez que os 57 assassinatos da Suíça não fazem a menor diferença e aumenta mais um país na lista, ou que o Brasil tem dimensões continentais e que a França, um dos maiores países da Europa, é do tamanho da Bahia, apenas o 5º maior estado brasileiro.

Então, comparemos com um continente inteiro, a Europa. Com 743 milhões de pessoas, o continente inteiro teve 22 mil assassinatos em 2015. O Brasil (com uma população mais de três vezes menor), teve quase o triplo.

Outra comparação que pode ser feita é a China que, com seu 1,3 bilhão de habitantes, registrou 10 mil homicídios em 2014, cabendo a ressalva de que os números oficiais são enganosos. Assassinatos ocorridos juntamente com roubo ou estupro podem ser descartados da estatística. Mesmo assim, os números chineses precisariam ser 36 vezes maiores para se equipararem aos brasileiros, no que se referente a taxa entre homicídios x população.

Observando de perto, a maioria dos países vão apresentar ressalvas devido as metodologias aplicadas, burocracias falhas, corrupção governamental. Contudo, mesmo duvidando dos dados, o Brasil está tão a frente nos números que fica difícil competir nesse ranking terrível. Em números absolutos, o país que mais se aproxima é a Índia, com 41,6 mil homicídios em 2014. O detalhe que desfavorece o Brasil, nesse caso, é que a Índia tem uma população seis vezes maior.

Cabe ressaltar, como já foi dito, que o Brasil tem dimensões continentais, e não dá pra generalizar e dizer que todo o Brasil é violento. Você pode morar no Jardim Paulista, em São Paulo, tão pacífico quanto a Suécia, ou em Nossa Senhora da Apresentação, o bairro mais violento de Natal, a cidade mais violenta do Brasil e a 10ª do mundo. Só no primeiro semestre de 2017, esse bairro registrou 40 homicídios. Em seis meses, somente esse bairro, teve mais assassinatos do que 66 países e territórios computados pelo UNODC (Deursen, 2018).

1.3. Portugal, um dos países mais pacíficos do mundo

De maneira oposta, temos Portugal, que é o quarto país mais pacífico do mundo, de acordo com o Índice Global da Paz de 2018 (Global Peace Index – GPI 2018) – uma classificação de 163 estados e territórios independentes de acordo com seu nível de tranquilidade, produzido pelo IEP (Institute for Economics & Peace, 2018) –, e a principal medida da tranquilidade global.

Apesar da sua queda de terceiro para quarto lugar no último ano, Portugal está entre os países com os melhores avanços na paz positiva desde 2013. Em 2013, Portugal ocupava a décima sexta posição (Institute for Economics & Peace, 2018).

O Brasil, por outro lado, ocupa a posição 106, a sua segunda pior posição desde que o ranking foi criado em 2008. No ano passado ocupava a posição 108. Além disso, registrou a pontuação máxima na taxa de homicídio (ECO, 2018).

A figura a seguir demostra o Índice Global da Paz de 2018, onde se pode observar que Portugal é um dos poucos países que possui a cor relativa às menores taxas de homicídio.

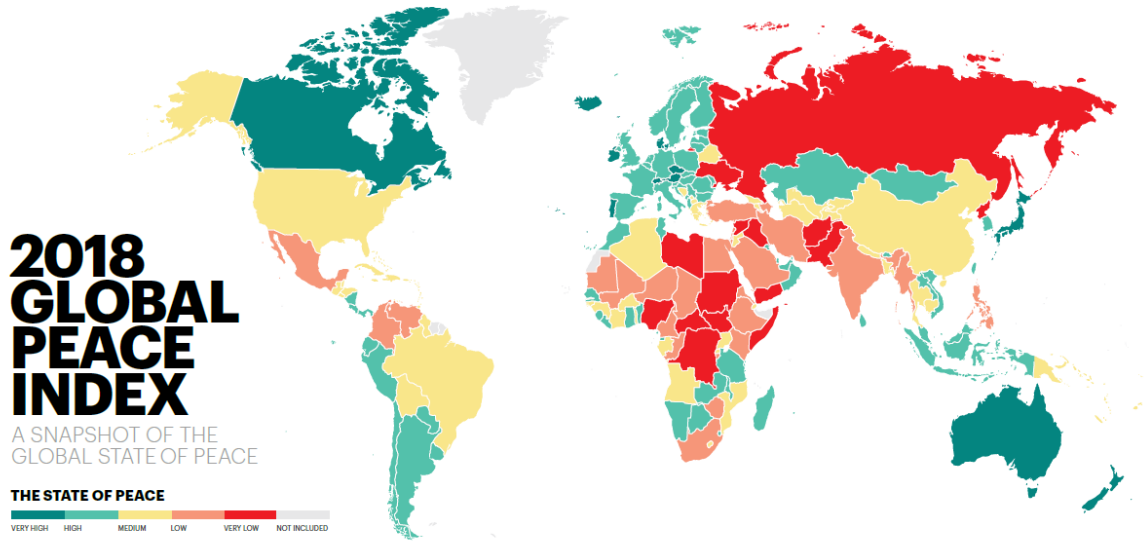

Figura 4: Índice Global da Paz de 2018 (Institute for Economics & Peace, 2018)

Nessa mesma linha, os EUA classificaram Portugal como um dos países mais seguros do mundo. O Departamento de Estado dos EUA tem um sistema de recomendações de segurança para viajantes com a classificação de risco de todos os países do mundo, agrupados em quatro níveis de ameaça. Nesse ranking, Portugal aparece como um destino seguro, classificado no 1º nível (o mais seguro em uma escala de 1 a 4), onde é recomendado apenas "precauções normais". A título de comparação dentro da Europa, países como Alemanha, França, Reino Unido, Itália, Bélgica e Espanha aparecem no 2º nível, devido ao

risco de ataques terroristas. O Brasil também é classificado no nível 2, com alertas de "áreas de alto risco de segurança" e para elevados níveis de criminalidade (Borges, 2018).

Segundo os dados divulgados pela UNODC (United Nations Office on Drugs and Crime, 2018), em 2016, houve 66 vítimas de homicídio intencional em Portugal, o que representa uma taxa de 0,6 homicídios intencionais a cada 100.000 habitantes.

O abismo que separa Brasil de Portugal é enorme, no que se refere aos riscos e ameaças à segurança pública, o medo da população e a preocupação dos cidadãos e estrangeiros com sua própria segurança. Não há dúvidas que, de acordo com os dados aqui apresentados e falando em traços gerais, pode se dizer que Portugal é um dos países mais seguros do mundo, e, de maneira oposta, o Brasil é um dos países mais violentos do mundo.

2. SOCIEDADE VIGILANTE

2.1. Breve história da identificação individual

Atestar a identidade de alguém de forma incontestável tem sido um desafio há muitos séculos, principalmente no âmbito criminal, para se apontar indubitavelmente o praticante do delito.

Diariamente utilizamos os nossos sentidos para identificar pessoas e coisas. Através da visão, olfato, paladar, audição e o tato somos capazes de reconhecer, comprovar e diferenciar pessoas e objetos do nosso dia a dia. Para Federico Olóriz Aguilera (apud de Araújo e Pasquali, [s.d.], p. 01) "a identificação é o ato mais frequente e elementar da vida social". Contudo, somente através de um método científico podemos imputar responsabilidade criminal a uma pessoa. Nesse sentido, importa diferenciar "identificação" de "reconhecimento".

Quando assistimos a uma partida de futebol, utilizamos a visão para diferenciar características dos jogadores e reconhecê-los. Em cursos policiais existe uma instrução de tiro onde os alunos aprendem a reconhecer o calibre de um armamento pelo som do disparo. Muitas vezes, enquanto aguardamos o almoço, reconhecemos o prato a ser feito através do olfato.

Assim, o reconhecimento nos traz a ideia de comparação, a identificação de algo com base em um banco de dados que se tem disponível, no caso dos exemplos trazidos, o banco de dados é a nossa própria memória e vivencias passadas.

Já para a "identificação" é fundamental o estabelecimento de uma identidade incontestável. Não é suficiente que os termos sejam parecidos ou semelhantes, é imperioso que sejam idênticos. No âmbito criminal, uma testemunha reconhece um suspeito como semelhante, mas cabe a polícia científica a obrigação de afirmar que tal pessoa é idêntica à que estava na cena do crime, a fim de imputar a responsabilidade do crime (Araújo e Pasquali, [s.d.]).

Quanto à identificação dos iindivíduos, é importante ressaltar que a preocupação com a atribuição de uma identidade invariável e facilmente verificável é levantada pelo impulso de individualização que agita o século XIX, o qual se manifesta através da estabilização de nomes (Garcia, 2008).

É nesse ambiente de individualização que começam a ser desenvolvidas as técnicas de identificação, que serão disponibilizadas ao poder estatal através da polícia, da medicina legal e da magistratura (Garcia, 2008).

Em um primeiro momento, os esforços dos Estados para desenvolver técnicas de identificação foram apontados para aquela parcela da sociedade considerada suscetível a gerar instabilidade social, ou seja, os criminosos. Nessa época, havia dificuldade na identificação de alguns criminosos que, como refere Peter Becker (2001, apud Garcia, 2008), para o caso da Alemanha, eram tidos como peritos no disfarce. Como exemplo da dificuldade de identificação dessa época, as fotos produzidas em algumas seções de polícia de Paris eram organizadas por nome; bastava que um criminoso se apresentasse com um nome falso para driblar esse sistema de identificação (Garcia, 2008).

Uma das primeiras técnicas de identificação foi a antropometria. Alphonse Bertillon (1853-1914) criminologista francês, define assim os princípios desse método: "todas as medidas humanas obedecem a uma lei natural de distribuição estatística; a escolha das características que devem ser medidas deve estar baseada na sua não-correlação, bem como na sua imutabilidade e clareza; a partir da medição de um número definido de ossos é possível fixar dados descritivos que identificam um indivíduo com alto grau de certeza" (Garcia, 2008).

A seguir à antropometria é desenvolvido um método mais promissor – a datiloscopia. Esse método é baseado em descobertas ancestrais das culturas japonesa e chinesa sobre como são dispostas as linhas papilares da mão. O anatomista tcheco Jan Evangelista Purkinje (1787-1869), através da classificação e agrupamento das curvas, arcos e círculos concêntricos das linhas da mão, descobriu a chave da variedade gráfica para a datiloscopia. Contudo, foi através dos estudos de Francis Dalton, primo de Darwin, que teve acesso à obra de Purkinje, que em 1891 foi inventado o primeiro método de indexação das impressões digitais (Garcia, 2008).

Em 1896, a datiloscopia é adotada como sistema único de identificação em La Plata, na Argentina, em 1897, na Índia britânica, em 1901, na Inglaterra e no País de Gales, em 1905, em Buenos Aires, Rio de Janeiro, Montevidéu e Santiago do Chile. Em 1907 é a própria Academia das Ciências francesa a reconhecer a superioridade do método, numa altura em que a datiloscopia era usada da América à Indochina, passando pela Europa, seguindo cerca de dez métodos diferentes (Mattelart, 1994, apud Garcia, 2008).

Além do estudo sobre datiloscopia, Francis Dalton é responsável por introduzir a ciência da eugenia. Proveniente do grego *eugeneía*, eugenia exprime "boa estirpe", "bom

nascimento" ou "profundamente ditado de qualidades nobres". Dalton defende que o cruzamento seletivo dos indivíduos, principalmente os de famílias favorecidas, seria capaz de interferir no processo de seleção natural a fim de aperfeiçoar os seres humanos como espécie. Por outro lado, deveria ser feito um controle de natalidade daquelas famílias menos favorecidas, para evitar a procriação de indivíduos menos talentosos (Garcia, 2008).

Apesar da não implementação das ideias de Dalton, é inegável o seu contributo para a ideia de que no âmbito biológico estaria alguma forma de identificação dos indivíduos, que é o prenuncio das aplicações criminalísticas da genética e do DNA na transição para o século XXI (Garcia, 2008).

O avanço científico dos métodos de identificação do século XIX foram, ao mesmo tempo, essenciais para o progresso dos direitos civis, políticos e das formas de proteção social, bem como, e paradoxalmente, essenciais para reforçar o poder de controle, vigilância e coação do Estado (Garcia, 2008).

2.2. Foucault e a sociedade contemporânea

É impossível falar de vigilância sem citar o filósofo francês Michel Foucault e sua celebre obra "Vigiar e Punir" (Foucault, 1999). Nessa obra, Foucault apresenta a teoria de uma sociedade disciplinar e expande a ideia do filósofo e jurista inglês Jeremy Bentham a respeito do Pan-óptico.

Nos séculos XVIII e XIX a sociedade passava por fortes mudanças sociais que levaram a alteração do jogo do poder, onde a sociedade disciplinar, denominação dada por Foucault, foi gradativamente substituindo a conjuntura de poder da época e atingiu seu ápice no início do século XX. O modelo em que se exercia o poder de forma rigorosa sobre aquele que transgredia a norma deu lugar a um modelo de vigilância generalizada, onde, através de mecanismos disciplinares, se visava a disciplina dos vigiados; percebeu-se que era mais eficaz e económico vigiar do que punir (Lopes e Santos, 2002).

Em seu estudo sobre o nascimento da prisão, Foucault reconheceu três fases distintas: inicialmente, nas sociedades soberanas do século XVII, a prisão existe junto com outras formas de punição, como o manicômio e o asilo. Com o declínio da soberania, a lei e o poder começam a regular a administração. Nesse momento acontece a estatização da Justiça Penal (Lopes e Santos, 2002).

Como observa Foucault, a prisão não é uma pena e direito do sistema penal dos séculos XVII e XVIII. Nessa época, o condenado devia uma reparação ao soberano, a lei e ao poder

monárquico, através de punições como a morte, ser queimado, esquartejamento, ser marcado, banido, pagar multa e etc (Lopes e Santos, 2002).

A seguir, no final do século XVIII e início do século XIX, e juntamente com a reforma e reorganização do sistema judiciário e penal, a prisão passa a se difundir pelos países da Europa e do mundo. Naquele tempo, a prisão se efetuava em um alto grau de disciplina, superando a imagem adquirida do período anterior (Lopes e Santos, 2002).

A esse período que Foucault intitula de "sociedade disciplinar", onde traz como características fundamentais a distribuição das pessoas em espaços individualizados, confinados, combinatórios, classificatórios, isolados, hierarquizados e capazes de desempenhar funções diferentes segundo o objetivo específico que deles se exige. Parte essencial desse modelo é a vigilância contínua, permanente e perpétua (Lopes e Santos, 2002).

Durante seus estudos sobre as prisões, Foucault se debruça sobre a arquitetura descrita por Jeremy Bentham em 1785 como "Pan-óptico", uma engenharia formulada para o domínio da distribuição de corpos em diversos espaços como a prisão, fábricas, escolas, manicómios e etc (Lopes e Santos, 2002).

Na prática, o Pan-óptico era um edifício circular, onde no meio havia um pátio com uma torre no centro. Em volta da torre, o edifício se dividia em pequenas celas vazadas, tanto para o interior quanto para o exterior. Dentro dessas "celas" poderia haver operários a trabalhar, alunos aprendendo a ler, prisioneiros cumprindo suas penas ou loucos a procura de cura, isso de acordo com o objetivo de cada instituição. Na torre central havia um vigilante (Lopes e Santos, 2002).

Do alto dessa torre, o vigilante podia ver tudo que se passava nas celas, uma vez que elas eram vazadas, e não havia nenhum ponto escuro que fugisse ao olhar do vigilante. Além disso, este observava os corpos através de persianas, de modo que a tudo podia ver, mas ninguém podia vê-lo (Lopes e Santos, 2002).

Ver sem ser visto, essa é a principal ferramenta do Pan-óptico. O essencial não era vigiar o prisioneiro em tempo integral, e sim que o prisioneiro soubesse que estava sendo vigiado. Dessa forma, a vigilância se torna permanente em seus efeitos, mesmo que não fosse em sua ação, e a garantia da ordem é alcançada. A finalidade do Pan-óptico não era punir as pessoas, mas antes evitar que elas cometessem o mal, pois se sentiriam permanentemente observadas (Lopes e Santos, 2002).

A ideia de um observador onipresente obviamente é uma ficção. Contudo, o Pan-óptico precisa simular essa onipresença para que os indivíduos permaneçam crentes de sua

existência. Para isso forja esse atributo através de rondas aleatórias, pela própria arquitetura do local, onde se é visto sem se ver e etc (Lopes e Santos, 2002).

Nesse cenário, o inspetor perfeito, o inspetor onipresente, é aquele que nunca é visto, mas que pode aparecer a qualquer momento. O Pan-óptico deve ser administrado por um olho e por uma voz desconectado do verdadeiro portador. Assim, o inspetor se torna uma espécie de ser místico, fictício. Essa ficção o torna mais temível que um guarda cruel, justamente por estar no imaginário dos observados (Lopes e Santos, 2002).

O panoptismo é a vigilância total do poder disciplinador sobre a vida de um indivíduo. É ser vigiado o tempo todo por alguém que não pode ser visto, e nem se pode saber em que momento está realmente a ser vigiado (Lopes e Santos, 2002).

As intensas transformações do século XX também trouxeram a mudança da sociedade disciplinar de Foucault, para a "Sociedade de Controle" explicada por Gilles Deleuze (1992). Atualmente se vive a sobreposição dos dois modelos, enquanto se caminha por essa transição. Estamos saindo de um modelo de confinamento completo das instituições para inserção da disciplina, para um controle difuso e constante (Lopes e Santos, 2002).

Enquanto na sociedade disciplinar o padrão Pan-óptico é dominante, onde é necessário a figura do observador vigiando os indivíduos, na sociedade de controle a vigilância é ampla e virtual. A sociedade disciplinar é fundamentalmente arquitetural: o prédio da escola, a casa da família, a fábrica, o quartel e etc. Em contrapartida, a sociedade de controle não tem muros, ela está em todo lugar (Lopes e Santos, 2002).

Importa destacar que o aspecto disciplinar também faz parte da sociedade de controle, apenas se altera a forma de atuação. As técnicas de poder que ficavam restritas aos espaços fechados das instituições se tornam mais fluídas e se espalham por todas as esferas sociais (Lopes e Santos, 2002).

Assim, o princípio do confinamento intramuros, uma das principais ferramentas para o exercício do poder, e até então, amplamente utilizada, deixa de ser essencial nas sociedades de controle. Já não existem fronteiras. Não existe o "dentro" e "fora". A realidade é que a lógica do confinamento, estimulada pela sociedade disciplinar, foi tão arraigada no corpo social que tornou possível, e até natural, a transição para uma sociedade de controle, onde já não são mais necessários os muros, o confinamento é global (Lopes e Santos, 2002).

Hoje em dia a vigilância é contínua e se efetiva através das câmeras de vigilância espalhadas por todos os lados: nos bancos, comércios, escolas e até mesmo nas ruas. A disseminação dos dispositivos tecnológicos e a facilidade de acesso tornou todos capazes de vigiar e ser vigiados. Todos podem e querem espiar a vida de todos. Trata-se da recriação do

Pan-óptico benthaniano, que opera de forma a transformar de maneira profunda o modo de pensar, viver e agir dos indivíduos.

Hoje é quase impossível sair de casa sem se deparar com placas que dizem: "sorria, você está a ser filmado". Sutil e gradualmente você está sendo constantemente vigiado por uma "instância superior", seja no elevador do seu prédio, na escola do seu filho, no seu trabalho, nos edifícios governamentais ou até nas ruas e praças públicas. E o objetivo é sempre o mesmo, vigiar, controlar e punir, conforme o caso, mas, essencialmente, controlar.

Essa vigilância constante que em um passado poderia incomodar, hoje já não constrange mais. Isso porque nós mesmos nos expomos constantemente nas redes sociais. Queremos ver a vida alheia e nos deixamos ser vistos, muitas vezes em busca de fama ou simplesmente a aprovação social.

A sociedade atual é descrita por Debord (2003) como a sociedade do espetáculo, uma sociedade que substitui a celebre frase do filósofo francês René Descartes "penso logo existo", por um outro pensamento que retrata melhor o mundo contemporâneo: "sou visto, logo existo" (Quinet, 2002, apud Lopes e Santos, 2002). A visibilidade e a transparência são inerentes à sociedade do espetáculo, e isso se vê refletido no aumento dos programas de televisão com exibicionismo explicito, bem como, na disseminação epidêmica de câmeras de vigilância.

Em suma, o principal objetivo da sociedade disciplinar era modelar o comportamento do indivíduo a partir do receio de que estivesse sendo vigiado pelo "observador". Na sociedade de controle observamos a incorporação da disciplina de tal forma que os indivíduos podem estar sob os efeitos das ferramentas disciplinares mesmo que não estejam na presença de uma autoridade capaz de impor os procedimentos de saber e de poder. A sociedade de controle expande e intensifica os fundamentos da sociedade disciplinar (Lopes e Santos, 2002).

2.3. Circuito Fechado de Televisão

Desde muitos séculos a sociedade utiliza a vigilância como forma de controle social. Como vimos no capítulo anterior, Foucault descreve essa vigilância através da sociedade disciplinar, que vigiava para garantir a segurança e o controle, nos mais diversos ambientes sociais como a fábrica, a escola, o presídio, o hospital, etc. Esse controle teorizado por Foucault, por vezes, é até intuitivo e básico da nossa sobrevivência, como uma mãe que vigia seu filho, para que este não sofra um acidente, ou a atitude vigilante de quando nos

encontramos em uma situação de perigo iminente. Vigiar, então, está na gênese da nossa sociedade, e a utilizamos, principalmente, para garantir a segurança.

Quando o Estado, enquanto organização social em prol do bem comum, escolhe vigiar seus cidadãos, essa vigilância tem a finalidade precípua de garantir a segurança pública e a paz social.

A vigilância do Estado se dá através de seus órgãos de controle e, principalmente, através dos órgãos policiais. As polícias, juntamente com o judiciário, sempre tiveram esse papel de vigiar a sociedade, para lhes garantir a segurança e punir àqueles com condutas desviantes.

A vigilância policial ocorre principalmente através do patrulhamento de seus agentes, seja a pé, em viaturas, motocicletas, helicópteros, a cavalo, etc. Essas modalidades utilizam o campo visual do agente para que ele possa perceber qualquer perturbação social enquanto cumpre a sua missão, e assim possa intervir imediatamente.

Contudo, essa vigilância nem sempre surte os efeitos desejados. O Estado, na figura do policial, não é onipresente. Ele não pode estar em todos os lugares ao mesmo tempo, obviamente, e, por isso, os crimes ocorrem. A ocorrência de crimes é considerada normal, não há sociedade sem crime. O que causa terror são os números já apresentados neste trabalho, em relação ao Brasil. Outro dado alarmante fornecido pela Estratégia Nacional de Justiça e Segurança Pública, é que, no Brasil, somente 6% dos homicídios dolosos (com intenção de matar) são solucionados no país (Coutelle, 2018). Ou seja, a vigilância não é importante somente no momento pré-crime, como também no pós-crime, devido a necessidade de se identificar o criminoso para aplicar a devida punição.

Diante da realidade atual de qualquer ramo social, onde se espera fazer mais com menos, pois os recursos estão cada vez mais escassos, enquanto as demandas são cada vez maiores, os Estados têm apostado em tecnologias para atingir os seus objetivos. É nesse cenário que as câmeras de videovigilância aparecem.

A videovigilância cresceu bastante devido à um caso emblemático no Reino Unido em meados dos anos 80, o triste e celebre caso do rapto e assassinato da criança de 2 anos, Jamie Bulger. Os autores do crime (na época também crianças, com 10 anos) foram identificados graças às câmeras de vigilância presentes no local. Esse caso fez se alastrar por todo o país a implementação de sistema de vigilância (Norris e Armstrong, 1999, apud Frois, 2008) (Norris, et al., 2004, apud Frois, 2008). E isso não foi uma exclusividade do Reino Unido, mas como mostra a revista *Surveillance & Society* sobre o tópico “The politics of CCTV in Europe and beyond” (2004), que, como indica o título, trata da proliferação de câmeras de

vigilância em países como a Noruega, a Dinamarca, a Áustria, a Alemanha, a Hungria, a França e a Irlanda, abrangendo ainda o Japão, a China ou a Austrália (Frois, 2008).

Mas o que é "CFTV" ou "CCTV"? CFTV é a sigla para Circuito Fechado de Televisão, que teve origem na sigla em inglês com o mesmo significado, o CCTV (*Closed Circuit Television*) (Central CFTV, 2019).

Na prática é um sistema de monitoramento realizado através de câmeras distribuídas e conectadas a um sistema central, que fornece imagens através de monitores, bem como faz a gravação desses registros. O CFTV é utilizado para o monitoramento e vigilância, sendo empregado nos mais diversos ramos como monitoramento viário, ambiental, segurança do trabalho, assim como, para a segurança púbica (Central CFTV, 2019).

As vantagens desse sistema é que uma equipe é capaz de monitorar, em tempo real e até remotamente, o que está acontecendo em vários ambientes simultaneamente, sendo capaz de tomar decisões e agir conforme a necessidade de cada caso que for detectado como anormal, e ainda, é capaz de passar informações valiosas aos agentes que estão em campo, devido a sua posição privilegiada (Central CFTV, 2019).

Além disso, o CFTV possibilita que as imagens registradas fiquem gravadas para serem analisadas e utilizadas posteriormente, auxiliando na identificação de criminosos e até sendo usadas como prova em processos legais. Outra vantagem acessória é a própria presença de câmeras no ambiente vigiado, que inibe a ação de criminosos ou pessoas mal-intencionadas (Central CFTV, 2019).

2.3.1. Crescimento do CFTV

A revista *Surveillance & Society* publicou em 2004 um artigo que demonstra o crescimento do número de câmeras de vigilância nos espaços públicos da Europa e pelo mundo (Norris, McCahill e Wood, 2004).

O artigo remonta ao estudo publicado pelo *Urbaneye Project* (Hempel e Töpfer, 2002), que documentou a proliferação das câmeras em espaços públicos e semipúblicos. Esses estudos foram realizados em seis capitais europeias e apontaram para o uso cotidiano do CFTV em espaços publicamente acessíveis, como lojas, bancos, restaurantes, bares, terminais de transporte, etc.

Em toda a Europa, 29% dessas instituições usavam alguma forma de videovigilância, embora, como mostra a Tabela 1, o crescimento foi desigual. Os dados do *Urbaneye* sugerem

que, em Londres, 40% dos espaços com acessos públicos foram monitorados por câmeras de vigilância, em comparação com apenas 18% em Viena (Hempel e Töpfer, 2004).

Apesar desses números indicarem a difusão geral do CFTV em toda a sociedade europeia, eles ocultam diferenças importantes entre a vigilância do espaço público e privado. Os dados do *Urbaneye* mostram que, em 2003, na Dinamarca e na Áustria, não havia sistema de CFTV em espaços públicos, havia apenas um na Noruega (que consistia em seis câmeras), pelo menos 14 sistemas em Budapeste e 15 na Alemanha. No Reino Unido, havia mais de 500 sistemas. Assim, enquanto no Reino Unido havia mais de 40.000 câmeras de CFTV monitorando o espaço público, provavelmente havia menos de 1.000 em todos os outros países europeus incluídos na pesquisa (Hempel e Töpfer, 2004).

Tabela 1 – Percentagem de vigilância em espaços com acesso público em seis capitais europeias e o número de sistemas de CFTV em espaços públicos em cada país

Cidade	% de instituições com câmeras em espaços com acesso público	País	Nº de sistemas de CFTV em espaços públicos
Londres	40	Reino Unido	Mais e 500
Oslo	39	Noruega	1
Copenhagen	33	Dinamarca	Nenhum
Budapeste	28	Hungria	Mais de 14, apenas em Budapeste
Berlim	21	Alemanha	15
Viena	18	Áustria	Nenhum

Fonte: Urbaneye, (Hempel e Töpfer, 2004): 27-34

Esses dados sugeriam uma expansão limitada do CFTV fora do Reino Unido. Contudo, em outros países europeus não incluídos no estudo do *Urbaneye*, houve um crescimento sustentado CFTV em espaços públicos. Na França, por exemplo, depois da flexibilização das leis sobre vigilância do espaço público em 1995, houve uma rápida implantação de CFTV nesses espaços. Entre 1997 e 1999, mais de 200 cidades francesas receberam a aprovação para a instalação de CFTV em locais de alto risco e 259 para a proteção de edifícios públicos, como prefeituras, bibliotecas públicas, escolas e museus (Hempel e Töpfer, 2002, apud Norris, McCahill e Wood, 2004).

Igualmente, na Holanda, as primeiras câmeras a serem usadas em espaços públicos ocorreu em 1997, e apenas seis anos depois, em janeiro de 2003, 80 dos 550 municípios do país estavam usando CFTV em locais públicos (Flight, et al., 2003, apud Norris, McCahill e Wood, 2004). Na Irlanda, o primeiro sistema de CFTV foi instalado em Dublin em meados dos anos 90, e expandido em 1997. Na época desse artigo de *Surveillance & Society*, o Ministro da Justiça Irlandês havia anunciado uma grande expansão CFTV de rua em todo o

país, com planos para estender a 21 áreas diferentes (Norris, McCahill e Wood, 2004). Na Itália, 22 das 33 instalações esportivas com capacidade para mais de 20.000 espectadores estavam equipadas com sistemas de videovigilância (Conselho da Europa, 2002, apud Norris, McCahill e Wood, 2004) e, naquela época, em resposta às ansiedades crescentes sobre o crime, o Ministério do Interior havia instalado CFTV nas áreas sensíveis de 50 cidades italianas (Norris, McCahill e Wood, 2004).

Nos EUA, a primeira pesquisa nacional de CFTV, realizada em 1997, descobriu que os departamentos de polícia de apenas 13 cidades do país usaram sistemas de vigilância CFTV, principalmente para tráfego de pedestres em bairros centrais e residenciais (Nieto, et al., 2002, apud Norris, McCahill e Wood, 2004).

Em 2001, cerca de 25 cidades dos EUA estavam usando CFTV para monitorar as áreas públicas; que variavam de pequenos sistemas como o sistema de CFTV do Balboa Park, em San Diego, com cinco câmeras monitorando o centro comercial e a área de museus, para sistemas muito maiores como em Washington/DC, que havia estabelecido o maior sistema público de vigilância por CFTV do país, ligando centenas de câmeras que monitoravam estações de transporte de massa, monumentos e escolas com novas câmeras digitais que vigiavam ruas, áreas comerciais e bairros (Nieto, et al., 2002, apud Norris, McCahill e Wood, 2004).

Apesar da pesquisa ter apontado para um avanço relativamente lento dos Estados Unidos em adotar tecnologias de CFTV, como na Europa, o crescimento predominante tinha sido no setor privado. Já em 1996, a pesquisa dos gastos dos negócios dos EUA feita por Hallberg descobriu que 75% das empresas usavam CFTV (Slobogin, 2002, apud Norris, McCahill e Wood, 2004).

Além disso, a preocupação com a segurança após o ataque terrorista de 11 de setembro de 2001, aliado aos avanços tecnológicos e os custos decrescentes dos produtos, levou à rápida difusão de vigilância por CFTV e tecnologias biométricas. Como exemplo, as câmeras de vigilância de CFTV são amplamente utilizadas nas escolas públicas para monitorar o movimento estudantil e identificar atividades ilegais, e ainda, em cruzamentos de rua para detectar carros atravessando sinais vermelhos (Nieto, et al., 2002 apud Norris, McCahill e Wood, 2004).

A pesquisa da Associação Internacional de Chefes de Polícia (*International Association of Chiefs of Police* – IACP, 2001) descobriu que, naquela época, 80% das agências de aplicação da lei nos EUA já utilizavam CFTV de alguma forma. Muitas forças policiais americanas tinham equipado suas viaturas com CFTV para monitorar a prisão e

procedimentos de detenção, e outros, tinham instalado em tribunais e outros edifícios do governo. Mas, mais da metade das agências que responderam também usavam CFTV em "áreas de alta criminalidade": 25% nas ruas, 15% em parques e pouco mais de 10% em locais de habitação pública (IACP, 2001, apud Norris, McCahill e Wood, 2004). Até mesmo antes de 11 de setembro, a pesquisa da IACP previa que a vigilância de CFTV estava pronta para crescer dramaticamente nos Estados Unidos.

Esses desenvolvimentos estavam refletidos nos números do valor e tamanho do mercado de CFTV nos Estados Unidos. Nessa época, o crescimento tinha acelerado desde o início dos anos 90, onde as receitas anuais da venda câmeras de vigilância mais que triplicam, indo de US$ 282 milhões em 1990 para mais de US$ 1 bilhão em 2000 (Norris, McCahill e Wood, 2004).

Atualmente, Londres é uma das cidades mais vigiadas do mundo – um relatório estima que o londrino médio é capturado por câmeras mais de 300 vezes por dia –, mas sua crescente rede de câmeras faz parte de uma tendência mundial. Em 2015, a indústria global de videovigilância foi avaliada em cerca de US$ 20 bilhões e deverá crescer para US$ 63,2 bilhões até 2022. Em 2014, havia 245 milhões de câmeras de vigilância instaladas profissionalmente ao redor do mundo (Teicher, 2018).

Na China, a efetivação do Projeto *Golden Shield* para criar uma infraestrutura de vigilância nacional levou à implantação de câmeras de vigilância por vídeo em uma escala sem precedentes (Norris, McCahill e Wood, 2004).

O projeto foi lançado para promover a adoção de uma avançada tecnologia de informação e comunicação para fortalecer o controle central da polícia, as capacidades de resposta e de combate ao crime, a fim de melhorar a eficiência e a eficácia da polícia (Walton, 2001).

O aparato de segurança da China anunciou um plano ambicioso: construir uma rede nacional de vigilância digital, ligando redes nacionais, regionais e agências locais de segurança com uma rede panóptica de vigilância. Pequim previu a *Golden Shield* como um sistema de vigilância remoto baseado em banco de dados, oferecendo acesso imediato aos registros de todos os cidadãos da China, ao mesmo tempo em que se liga a uma vasta redes de câmeras projetadas para aumentar a eficiência policial (Walton, 2001).

Os efeitos dessa política começavam a ser vistos em cidades da China. Em julho de 2004, o escritório de Segurança Pública de Hangzhou anunciou planos para instalar mais de 1.000 postos de observação através da cidade, cada um equipado com câmeras de segurança CFTV. De acordo com uma notícia de jornal da época, seria dada uma atenção especial a

grandes shoppings, praças, teatros, locais de entretenimento, estações de transporte, hotéis e em lugares que ainda não estavam em um estado de ordem adequado (Norris, McCahill e Wood, 2004).

Funcionários afirmavam que o esquema teria sido motivado por crescentes preocupações com o crime de rua e as seis primeiras centenas de postos de observação custariam US$ 12 milhões (China Daily, 2004, apud Norris, McCahill e Wood, 2004). Da mesma forma, em agosto de 2004, autoridades da cidade de Xangai revelaram planos para ampliar a pequena rede de câmeras existente, onde, de acordo com um relatório da época, até 2010, planejavam instalar mais de 200.000 câmeras de CFTV em toda Xangai, a fim de deter o crime e manter ordem social (Straits Times, 2004, apud Norris, McCahill e Wood, 2004).

2.3.2. Tendência de crescimento do CFTV

Essa propagação global da vigilância por CFTV mostrou uma tendência geral de crescimento dessa tecnologia nos países em quatro fases distintas, sendo elas (Norris, McCahill e Wood, 2004):

1ª Fase: Difusão privada

O CFTV se solidifica no setor privado, particularmente nos bancos e centros comerciais, como uma forma de impedir roubos, furtos, fraudes e supervisionar o espaço semipúblico. Esses sistemas tem a tendência de ser pequeno e pouco sofisticado, consistindo em câmeras fixas com pouco tempo de gravação, sendo que, muitas vezes, não há pessoal dedicado ao monitoramento contínuo das câmeras.

2ª Fase: Difusão institucional na esfera pública

Percebe-se a difusão do CFTV em instituições-chave da infraestrutura pública, particularmente em meios de transporte, escolas, edifícios governamentais e áreas de importância simbólica local. Fora do setor de transportes, muitos desses sistemas são tecnologicamente simples, com câmeras fixas e rastreamento limitado, mas com capacidades facilitadas por câmeras pan-tilt (panorâmicas/inclinação) e zoom. Muitos não têm pessoal dedicado para monitoramento contínuo do sistema.

3ª Fase: Difusão limitada no espaço público

O CFTV passa para o espaço totalmente público da cidade, justificadas principalmente pela sua capacidade de dissuadir e detectar o crime. Estes sistemas são comprados com

dinheiro público e são geralmente geridos por autoridades municipais ou polícias locais. Essa fase geralmente começa com sistemas de pequena escala, focados em problemas locais da área central da cidade e em áreas de lazer. Os sistemas variam em tecnologia e organização, indo desde sistemas com câmeras fixas, que não são monitoradas continuamente a sistemas mais sofisticados, com um grande número de câmeras pan-tilt e zoom totalmente funcionais, com potencial de gravação das imagens em tempo real que alimentam uma sala de controle centralizada, com pessoal dedicado ao monitoramento continuo e com comunicação direta para a segurança ou polícia local, que podem ser mobilizados para lidar com incidentes específicos.

4ª Fase: Em direção à onipresença

A fase final nos traz a criação de sistemas muito maiores, com centenas de câmeras que cobrem todas as áreas de uma cidade. E ainda, existe uma tendência para a integração de sistemas em larga escala, com sistemas menores pré-existentes, tanto públicos como privados, sendo interligados a uma central de monitoramento. Esses sistemas são capazes de fornecer todo um conjunto de funções auxiliares, tais como controle de tráfego, controle de acesso e, cada vez mais, utilizam tecnologias que permitem o automático reconhecimento facial ou de placas veiculares e que estão ligados a bases de dados informatizadas a nível local ou nacional.

Essas são as quatro fases identificadas no artigo de Norris, et al. (2004), de uma análise do crescimento dos sistemas CFTV em vários países. Obviamente que não é uma sequência imutável e determinista a ponto de dizer que um primeiro passo leva ao estágio final. A progressão das fases, e até o início da primeira, depende de fatores complexos, e da interação entre eles, de cada país e sociedade. Fatores socioeconômicos, legais, fiscais e políticos podem paralisar ou impulsionar a progressão dessas fases (Norris, McCahill e Wood, 2004).

Segundo o artigo, as evidências sugerem que o CFTV está pronto para se tornar uma 'Quinta Utilidade' global (Graham, 1998, apud Norris, McCahill e Wood, 2004) e que, apesar de haver diferentes taxas de crescimento da utilização do CFTV nos diversos países, gradualmente, se tornará “onipresente”. Nos diferentes países do mundo é comum ver um momento que desencadeia o clamor social para a extensão da videovigilância, podendo ser o sequestro de uma criança, um assassinato em sala de aula, um ataque terrorista ou a crescente preocupação com a criminalidade. Por exemplo, no Reino Unido, nos EUA e na Rússia, a resposta aos assassinatos em salas de aula tem sido a introdução generalizada de

CFTV no sistema público de ensino (McCahill e Norris, 2002; Time Europe, 2004; Nieto, 1999; apud Norris, McCahill e Wood, 2004). Normalmente, quando tais crises ocorrem, a emoção prevalece sobre a razão, e as soluções mais rápidas são postas à mesa. No final, equilíbrio entre liberdades civis e segurança terá que ser inclinado em favor da segurança (Norris, McCahill e Wood, 2004).

2.3.3. Tipologias de câmeras CFTV

Com base em um estudo realizado no sistema de câmeras CFTV da principal estação de trem de Zurique, e a maior estação ferroviária da Suíça, Christoph Müller e Daniel Boos (2004) apresentam quatro tipologias de sistemas CFTV, que levam em consideração as motivações para a instalação das câmeras, suas funcionalidades e seus efeitos sobre os passageiros e clientes, sendo elas: (1) controle de acesso, (2) controle de conduta, (3) registro de evidências, (4) controle de fluxo e o planejamento de intervenções. Segundo os autores:

Tipo 1: controle de acesso

O controle de acesso é um dos propósitos mais antigos para instalação de câmeras que observam espaços públicos. Elas são utilizadas para fiscalizar as pessoas não autorizadas que acessam locais proibidos. Normalmente são colocadas em entradas – de uma casa, de um banco, de um ambiente de alto risco como prisão ou usina nuclear – ou em fronteiras de países. Elas podem ser visíveis ou ocultas. Podem registrar todos os movimentos ou apenas quando alguém solicita permissão para acesso em uma determinada área. Na maioria dos casos, essas câmeras não gravam as imagens. No entanto, caso essas câmeras gravem o controle de acesso, essas imagens podem ser usadas posteriormente como evidência para aplicação da lei (ver tipo 3 abaixo).

Importa anotar que essas câmeras não bloqueiam o acesso por si mesmas. Elas funcionam como: (a) uma ferramenta de apoio para o pessoal que monitora o acesso a fim de para auxiliar na tomada de decisão de permitir ou negar o acesso e/ou, principalmente; (b) como um símbolo para uma autosseleção de acesso. De fato, as câmeras podem ter uma função dissuasora, ainda mais quando elas são visíveis e têm sua presença sinalizada, como: “Cuidado: se você não tem permissão para entrar nessa área, é melhor você sair…”. Nesses casos, as câmeras funcionam como símbolos e sinais, podendo, inclusive, ser substituídas por manequins (câmeras falsas).

Tipo 2: controle de conduta

Uma vez que o acesso é livre, as câmeras podem ser utilizadas para lembrar os usuários de certas 'regras de conduta' do local. No exemplo da estação ferroviária de Zurique, e como é comum em outros sistemas de mobilidade urbana pelo mundo, existem sinais que informam as regras da estação, principalmente os 'não faça', como: não corra, não ultrapasse a linha amarela, não pule nos trilhos do trem, etc.

Dessa forma, as câmeras também podem ser utilizadas com o mesmo propósito simbólico, principalmente quando são visíveis e sinalizadas. Esse é um aspecto importante do controle social das câmeras: Elas estão lembrando as pessoas que elas estão sendo vigiadas – ou para ser mais preciso, as câmeras dão às pessoas a impressão de que elas estão sendo vigiadas – e que elas devem se comportar bem.

Importa ressaltar que esse efeito de prevenção das câmeras não é direcionado somente para aqueles indivíduos que tendem a ter desvios de conduta, mas sim para todos, incluindo seguranças e a própria polícia. Por exemplo, as câmeras colocadas na área de venda de ingressos na estação de trem não são destinadas apenas para evitar roubos, além disso, lembram os assistentes de venda que eles estão sendo observados e não devem cometer furtos, e ainda, e muitas vezes como objetivo principal, que eles devem tratar bem os clientes e serem educados. Essa função de lembrar como as pessoas devem se comportar traz um valor simbólico para as câmeras, assim como no caso do controle de acesso. Elas aumentam a conscientização em espaços públicos por meios simbólicos.

Assim, as câmeras têm um efeito positivo, efeito de estímulo, de reforçar condutas desejáveis e o efeito negativo, efeito desestimulante, de reforçar a autorrestrição e a autodisciplina. E isso vai de encontro ao mecanismo do Pan-óptico descrito por Foucault, onde os vigiados podem ser constantemente observados, mas nunca sabem se são realmente observados. Isso pode levar a um aumento da consciência e para adaptações de comportamento. Enquanto os clientes da estação ferroviária acreditam que podem ser observados, eles podem adaptar seu comportamento como se estivessem sendo observados. Essa é uma forma geral de "dissuasão" e de "controle de conduta".

Subtipo 2: 'Sentir-se seguro' e aumentar a conscientização

A prevenção bem-sucedida da ordem social, resultando em reduções nos riscos de comportamento inesperado, pode levar a uma sensação geral de estar em um ambiente seguro. Isso pode ser encarado como um subtipo de controle de conduta. Se a disciplina social é incentivada com sucesso através de câmeras que funcionam como sinal, e a

consciência aumenta, então os clientes e funcionários podem se sentir seguros, porque, se as pessoas agem bem, isto é, na forma como se é socialmente esperado que elas ajam neste lugar e no tempo, o espaço é percebido como controlado, silencioso e protegido. Obviamente que essas câmeras não são o único meio que leva essas pessoas a se sentirem seguras, mas sim a combinação de outros meios que incluem o projeto arquitetônico, iluminação, uso de materiais "amigáveis" e brilhantes, assim como outros símbolos e sinais.

Contudo, este tipo de função simbólica do CFTV é baseada em uma série de pressupostos: elas só funcionam como um meio de controle de conduta se as pessoas acreditarem que as câmeras são reais (e não manequins), que elas estão funcionando corretamente, que estão sendo monitorados por alguém, que este "alguém" é capaz de organizar uma intervenção, se necessário, ou pelo menos que as imagens registradas podem ser usadas como evidência de sanções posteriores.

Tipo 3: registrando evidências

Tanto nas câmeras de controle de acesso (tipo 1) quanto nas de controle de conduta (tipo 2), a conduta "errada" pode ser sancionada, por exemplo, ao entrar em uma área sem permissão, ou ao se comportar maneira "inapropriada", talvez até de maneira criminosa. Para sancionar tal comportamento, provas ou evidências são necessárias. Se as imagens de uma câmera forem gravadas, essas imagens poderão ser utilizadas como evidências ou mesmo como provas, eventualmente levando a sanções como punição. Se as imagens não são registradas, mas foram monitorados por pessoas, então essas pessoas podem agir como testemunhas.

Um exemplo típico de câmera utilizada para registrar evidências são as câmeras instaladas próximas a caixas eletrônicos (ATM), onde, toda vez que alguém inicia uma interação ou transação com a máquina, uma foto do usuário é capturada e gravada. Em casos de fraudes essa imagem pode ser utilizada como evidência.

Muitas câmeras são usadas para coletar evidências, especialmente ao gravar imagens sem monitoramento em tempo real. Exemplos típicos de câmeras para coletar evidências são focadas em: (a) furto, roubo e fraude; (b) vandalismo e dano à propriedade; (c) ataques pessoais; (d) "terror" (no sentido de ameaçar o público). Nesses casos, as câmeras são mais que simples sinais, mais do que lembretes, elas são instrumentos, ferramentas. A evidência pode ser usada para planejar uma intervenção (ver tipo 4) ou para sanções posteriores.

Câmeras deste tipo não excluem os dois primeiros tipos, pelo contrário, elas podem ser usadas para reforçar o aspecto simbólico e apelativo das câmeras utilizadas como sinais,

bem como, as pessoas podem esperar que as imagens estão sendo gravadas e evitar a área que está observada ou adaptar seu comportamento. A gravação pode ser uma função a mais dos dois primeiros tipos de câmera.

Tipo 4: controle de fluxo e planejamento de intervenções

O quarto tipo de câmera é utilizada para o planejamento de intervenções. Talvez esta seja a forma mais antiga de vídeo vigilância de locais públicos. Esse tipo de câmera é utilizado desde o início dos anos 50 para controlar o tráfego de carros, especialmente em túneis. Quando, em um determinado cenário, "algo dá errado" ou sai de ordem, câmeras e sistemas de CFTV podem ser instrumentos úteis no planejamento de intervenções. No caso da principal estação de ferrovia de Zurique, este parece ser o principal objetivo do sistema CFTV. Quando acontece incêndios ou grandes acidentes, por exemplo, é importante saber quais acessos devem ser fechados, quais acessos estão abertos para as brigadas de incêndio, bombeiros, ambulâncias, etc.

Esse tipo de câmera também pode ser utilizado de forma preventiva, por exemplo, para observar o fluxo de uma torcida organizada ou manifestações. O princípio básico das câmeras de CFTV usadas para este tipo é o controle de fluxo. O monitoramento não precisa levar necessariamente a intervenções, mas deve ser visto como uma ferramenta de comando e controle para o planejamento de intervenções e sanções. Quando os incidentes são detectados, as câmeras podem ser usadas para coordenar a resposta.

Uma característica importante para o planejamento e coordenação de uma intervenção através da utilização desse tipo de câmera é a transmissão em tempo real das imagens coletadas pelo sistema CFTV. As imagens não precisam necessariamente serem gravadas, pois o foco principal é no coletivo, em multidões, e não em indivíduos.

Obviamente que esse catálogo de tipologia das câmeras não esgota todos os tipos possíveis e finalidades disponíveis que se têm no mercado, principalmente com a evolução contínua dessa tecnologia, mas é uma categorização importante e útil para saber quais funcionalidades e qual a finalidade se deseja atingir quando se planeja a aquisição de câmeras e sistemas CFTV.

2.3.4. Efetividade do sistema CFTV

2.3.4.1. Estudos de casos na África do Sul

O uso e a implementação de sistema de vigilância CFTV nos espaços públicos da África do Sul foi objeto de um estudo com a proposta de se verificar o impacto causado no controle do crime (redução dos índices criminais) e na prevenção criminal. Foram realizados estudos de casos de sistemas de CFTV instalados nos Distritos Comerciais Centrais (DCC) de quatro cidades sul-africanas: Cidade do Cabo, Joanesburgo, Pretória e Durban (Minnaar, 2007). Este tópico é baseado nos resultados desses estudos de casos.

O estudo revelou uma redução considerável nos crimes denunciados nos DCC onde foram instalados. No estudo de caso realizado na Cidade do Cabo, o sistema não só substituiu a utilização de 450 policiais patrulhando a DCC por 25 policiais em três turnos de oito horas (uma considerável economia de mão-de-obra e custos), como também, no primeiro ano de funcionamento do sistema completo de 75 câmeras, levou a uma redução de 38% dos crimes reportados na área (apenas o DCC central) com uma redução prevista de 80% até o final do segundo ano (Penberthy, 2001, apud Minnaar, 2007).

No primeiro ano de funcionamento, o sistema de CFTV do DCC de Joanesburgo havia relatado uma queda de 90% em assaltos na área, enquanto todos os crimes relatados diminuíram em 48%.

No final de 2001, as 200 câmeras instaladas em torno de todo DCC de Joanesburgo ajudou a reduzir a criminalidade em 80%. Além disso, o impacto positivo adicional desta redução foi que os preços de seguro para os negócios caíram, o aluguel de propriedades da qualidade do DCC se firmou e as empresas retornaram ao centro da cidade.

Uma aplicação comercial bem-sucedida foi a instalação de CFTV em todas as filiais do *First National Bank* no centro da cidade de Joanesburgo. Nos 12 meses anteriores à instalação do sistema de CFTV, ocorreram nove assaltos a filiais do banco, resultando em milhões de Rands (moeda local) roubados. Nos doze meses seguintes ocorreu apenas um roubo, sendo que os autores foram posteriormente detidos e o dinheiro recuperado. Quatro dos cinco assaltantes foram capturados e processados devido às evidências fornecidas pelas gravações de vídeo das câmeras de CFTV.

Até o final de janeiro de 2003, o sistema de vigilância CFTV do DCC de Johannesburg (então com um 184 câmeras instaladas) supostamente teve um impacto significativo sobre o crime. O número total de crimes relatados no DCC de Joanesburgo reduziu 80%, sendo que

os crimes graves e violentos reduziram em 75% e os crime não graves em 90% (Cox, 2003, apud Minnaar, 2007).

Em janeiro de 2006, Cueincident (a empresa responsável pela instalação das câmeras) afirmou que não houve um assalto a banco bem-sucedido no centro da cidade de Joanesburgo desde 2002, quando um total de 178 câmeras CFTV tinham sido instaladas. Além disso, foi afirmado que, durante esse período, um total de cinco assaltos a bancos foram frustrados (Cox, 2006, apud Minnaar, 2007).

No DCC de Pretória/Tsuane, o sistema, lançado em dezembro de 2004, gerou um sucesso imediato, com 50 prisões ocorridas entre 21 de dezembro de 2004 e 4 janeiro de 2005 – tudo atribuído às novas câmeras. Além disso, a Polícia Metropolitana de Tsuane recuperou dois veículos roubados e prestou assistência à 236 incidentes e infrações rodoviárias durante o mesmo período. As autoridades de Tsuane afirmaram que as câmeras tiveram um efeito positivo na prevenção do crime na cidade (Hlahla, 2005, apud Minnaar, 2007).

A redução da criminalidade continuou em Pretória/Tsuane e, nos primeiros seis meses de operação (21 de dezembro de 2004 a 1 Junho de 2005), um declínio de aproximadamente 30% ao mês dos relatos de crimes de rua e, em Junho de 2005, Cueincident assegurou que o crime de rua no centro da cidade tinha diminuído mais de 80%, enquanto houve quase 100% de redução dos assaltos a bancos.

Reduções semelhantes na criminalidade foram relatadas depois que o sistema de vigilância de frente para a praia de Durban foi expandido e modernizado no início de 2005, onde o sistema (em conjunto com policiamento privado e público) recebeu o crédito de ter reduzido os níveis de crime em até 35% na área da orla (Cole, 2005, apud Minnaar, 2007).

O autor do artigo ressalta que as alegações de redução da criminalidade acima expostas não devem ser aceitas incondicionalmente e sem crítica. Apesar dos operadores de CFTV e do gerente operacional dos sistemas de Joanesburgo e Tsuane serem inflexíveis em afirmar que os sistemas têm, indubitavelmente, reduzido o crime de rua visível e ajudou na redução de certos crimes violentos, tais como sequestro em veículos e assaltos a banco nos DCCs.

Contudo, as reduções reivindicadas, por exemplo, pela empresa Cueincident, são baseadas em suas próprias estimativas ao comparar os incidentes registrados desde que o sistema começou a operar em 2001. Infelizmente não se baseiam em nenhuma análise abrangente ou científica de crimes registrados e estatísticas dos Serviços Policiais sul-Africanos.

Mesmo assim, do que foi estudado, pode-se dizer que os quatro sistemas de vigilância CFTV sul-Africanos parecem ter um número interessante de inovações ou boas práticas como indicadores para a implementação operacional em outras partes da África do Sul, especificamente o fato de serem sistemas tecnologicamente avançados, fazendo uso da mais recente tecnologia disponível e de equipamentos com renovação constante. Além disso, as salas de controle operadas pelo Cueincident dispõem de um controle central com monitoramento e vigilância 24/7 e ligados diretamente às equipes de resposta da polícia (esse monitoramento é apoiado por um programa de treinamento especializado).

Todos os quatro estudos de caso descritos acima resultaram de iniciativas de planejamento, instalação e operação do setor privado. Além disso, todos os quatro estudos de caso têm sistemas operacionais consideráveis (pelos padrões sul-africanos) com pelo menos 200 câmeras por sistema. Embora não existam sistemas exclusivamente policiais, operados ou administrados, na África do Sul, todas esses sistemas têm um foco na redução/prevenção da criminalidade (essencialmente no "policiamento em parceria") com a presença e rápida resposta/reação da própria polícia em cooperação com os operadores das salas de controle e, em determinadas circunstâncias, a assistência de guardas municipais de segurança privada.

Além disso, o sistema Cueincident também está focado em manter a integridade das imagens de vídeo (gravações duplas - algumas digitais, frequentes mudanças de fitas e arquivamento) para que possam ser usadas como prova em um tribunal e ajudar procuradores a alcançar processos bem-sucedidos. As melhores salas de controle têm um suporte melhor devido a um abrangente programa de treinamento para os operadores, em particular na observação e habilidades de monitoramento.

Os números apresentados nesse estudo sul-africano são impressionantes, apesar de haver críticas quanto a recolha e fidelidade dos dados. O certo é que essa tecnologia veio para ficar na África do Sul. A questão agora é se as cidades menores do país serão capazes de custear essa tecnologia e se as futuras implementações continuarão a surtir o mesmo impacto na redução dos índices criminais (Minnaar, 2007).

2.3.4.2. Relatório CFTV e a prevenção criminal

Outro importante documento no campo de estudo da efetividade dos sistemas de câmeras CFTV é o relatório *CCTV and Crime Prevention* (Piza *et al.*, 2018), que atualiza as revisões sistemáticas e meta-análises do efeito de prevenção do crime através de circuito

fechado de televisão de (CFTV) conduzido por Welsh e Farrington (2002, 2007, 2009). Este tópico é baseado nos resultados apresentados por esse relatório.

O relatório adicionou 36 novas avaliações de CFTV que atendiam aos critérios de inclusão, e somados aos 44 estudos presentes na última revisão (Welsh e Farrington, 2007, 2009), esse relatório contêm 80 avaliações de CFTV. Dos 80 estudos, 76 forneceram os dados necessários para serem incluídos na meta-análise.

Com a evolução tecnológica dos sistemas e o aumento de sua implementação pelo mundo a quantidade de conhecimento científico sobre CFTV tem aumentado constantemente. Este relatório identificou 80 estudos que atenderam aos critérios de inclusão, resultando em um melhor conhecimento dos efeitos do CFTV. A quantidade de novas pesquisas conduzidas em CFTV em áreas residenciais ilustra essa questão. Enquanto a revisão anterior incluía apenas duas avaliações de CFTV nessas áreas, esta revisão identificou 14 estudos adicionais que atenderam aos critérios de inclusão. Isso tornou as áreas residenciais o segundo cenário mais comum para avaliações de CFTV (16 estudos), atrás de cidade e centros urbanos (33 estudos).

Além disso, enquanto as avaliações do Reino Unido eram a maioria (82,93%) dos estudos da última versão, nesta nova revisão as avaliações do Reino Unido representaram menos da metade (44,74%) dos estudos. O campo agora tem muito mais evidências sobre o efeito de CFTV em outros países.

Os resultados deste novo relatório apoiam e constroem as lições da última revisão (Welsh e Farrington, 2007, 2009). Por um lado, os efeitos combinados mostram que o CFTV está associado a uma modesta, mas estatisticamente significativa, redução do crime.

O relatório apontou para uma redução geral de 13% no crime, que é similar aos 16% de redução de encontrados por Welsh e Farrington em 2007 e 2009. Semelhante à revisão anterior, também foram encontrados efeitos maiores e mais consistentes de CFTV dentro dos parques de estacionamentos.

Por outro lado, enquanto Welsh e Farrington (2007, 2009) apontaram os estacionamentos como os únicos cenários onde o CFTV foi associado com efeitos significativos, a nova revisão encontrou provas de reduções significativas do crime em outras situações, mais notavelmente em áreas residenciais. Contudo, as evidências de redução de crimes não foram tão estáveis em áreas residenciais como nos parques de estacionamentos.

Assim como na revisão anterior, esse novo relatório reforça a ideia de que a implementação de outras intervenções ao lado do CFTV intensifica a efetividade da videovigilância. Foi observado que esquemas que incorporaram múltiplas intervenções com

o CFTV geraram melhores efeitos do que esquemas com intervenções únicas ou apenas com o CFTV.

Essa afirmação corrobora com a ideia de que o efeito de CFTV é maximizado quando a tecnologia é considerada uma componente chave de um pacote de intervenções, e não como uma tática autônoma contra o crime (La Vigne, et al., 2011; Piza, et al., 2015, apud Piza, et al., 2018).

Além disso, os sistemas de CFTV monitorados ativamente geram reduções significativas da criminalidade, enquanto sistemas passivos não tem efeitos significantes. Mais uma vez o argumento contra o uso isolado do CFTV como tática de prevenção da criminalidade é fortalecido, isto é, a simples presença visível da câmera pode não gerar o efeito dissuasivo pretendido, para isso, é necessário o monitoramento ativo das câmeras e a subsequente resposta de prevenção ao crime ante o fato gerador.

Por fim, os resultados da nova revisão foram semelhantes aos de Welsh e Farrington (2007, 2009) no que se refere ao uso de CFTV no Reino Unido, onde os 34 estudos demonstraram uma redução significativa de 10% nos índices criminais das áreas experimentais. E ainda, esta revisão encontrou redução de criminalidade em estudos da Coreia do Sul, apesar de serem apenas três estudos, 9% das avaliações realizadas no Reino Unido.

Cabe ressaltar, também, a constatação da falta de efeitos significantes dos sistemas CFTV nos estudos dos EUA, mesmo a nova revisão adicionando 20 novos estudos sobre o país, efeito que já havia sido observado por Welsh e Farrington (2007, 2009). Nesse estudo, Welsh e Farrington atribuíram essa observação ao fato de que o Reino Unido incorporava mais intervenções suplementarem do que em outros países, o que lhes trazia uma efetividade maior no uso dos sistemas CFTV.

Contudo, para a nova revisão, essa diferença não foi tão grande, pois 64,71% dos esquemas estudados no Reino Unido incluíam outras intervenções, enquanto nos EUA foram 57,17%. Outro fator que pode explicar a diferença de efetividade é a diferença de contextos culturais, uma vez que existe um alto nível de suporte para o CFTV no Reino Unido (Norris e Armstrong, 1999; Phillips, 1999, apud Piza, et al., 2018). Como argumentado por Welsh e Farrington (2007, 2009), isso pode significar que o apoio político e público necessário para maximizar os efeitos do CFTV pode estar ausente nos EUA.

Para concluir e resumir as descobertas do estudo, seguem seus principais achados (Piza *et al.*, 2018):

• No geral, o CFTV está associado a uma modesta, mas significativa redução do crime;

• O efeito do CFTV foi maior e mais consistentemente observado em estacionamentos. No entanto, as descobertas sugerem que mais configurações podem utilizar efetivamente o CFTV do que se pensava anteriormente, como a redução da criminalidade observada em áreas residenciais;

• Dos seis países onde foi avaliado, o CFTV mostrou a mais forte evidência de eficácia no Reino Unido;

• Dos cinco principais tipos de crimes testados nas avaliações de CFTV, os crimes de propriedade, de veículo e de drogas exibiram as reduções estatísticas mais significativas;

• A forma como as agências de segurança pública usa o CFTV é uma consideração importante. Sistemas monitorados ativamente e programas de implementação do CFTV em conjunto com várias outras intervenções geraram melhores efeitos do que suas contrapartes.

Por fim, destaca-se que o Relatório de Conjuntura com o título "Custos Econômicos da Criminalidade no Brasil", publicado em junho de 2018 no Brasil, apontou a utilização de Circuito Fechado de Televisão para prevenção e investigação de atividades criminosas como uma intervenção em segurança pública com impacto significativo na redução de crimes contra propriedade, inclusive com evidências científicas (Secretaria-Geral da Presidência do Brasil, 2018).

2.4. Reconhecimento Facial

2.4.1. Como funciona

Os seres humanos sempre foram capazes de reconhecer e diferenciar rostos, uma forma de interação inata da nossa espécie. Por outro lado, os computadores começaram a demonstrar essa capacidade recentemente. Em meados da década de 1960, os cientistas começaram a explorar o uso de computadores para reconhecer rostos humanos. Desde então, os programas de reconhecimento facial evoluíram bastante (Bonsor e Johnson, 2001). Este tópico é baseado no artigo escrito por Bonsor e Johnson (2001).

A empresa Identix, sediada em Minnesota, é uma das muitas desenvolvedoras da tecnologia de reconhecimento facial. Seu *software*, o FaceIt, pode selecionar o rosto de alguém em uma multidão, extrair o rosto do restante da cena e compará-lo a um banco de dados de imagens armazenadas. Para que esse *software* funcione, ele precisa saber diferenciar um rosto do restante do plano de fundo. O *software* de reconhecimento facial é baseado na capacidade de reconhecer um rosto e, em seguida, medir as várias características desse rosto.

Cada rosto tem inúmeros marcos divisórios distintos, os diferentes picos e vales que compõem as características faciais. FaceIt define esses pontos de referência como pontos nodais. Cada rosto humano tem aproximadamente 80 pontos nodais. Alguns destes, medidos pelo *software*, são:

- Distância entre os olhos;
- Largura do nariz;
- Profundidade das órbitas oculares;
- A forma das maçãs do rosto;
- O comprimento da linha da mandíbula.

Esses pontos nodais são medidos criando um código numérico, chamado *faceprint*, representando a face no banco de dados.

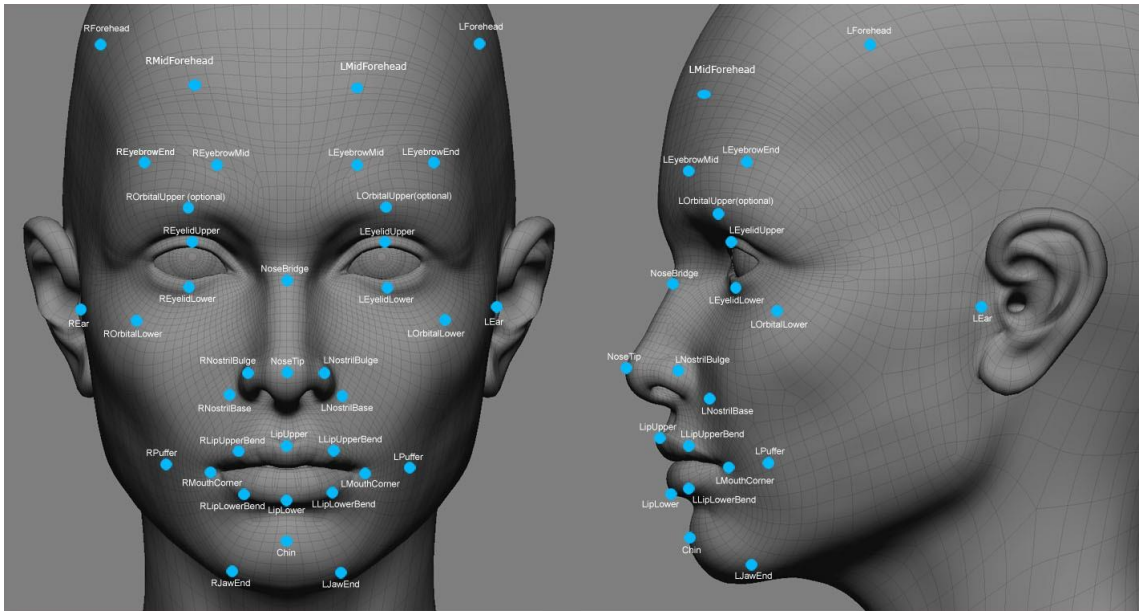

Figura 5: Pontos nodais em uma face (DEVFUN LAB, 2017)

No passado, o *software* de reconhecimento facial dependia de uma imagem 2D para comparar ou identificar outra imagem 2D do banco de dados. Para ser eficaz e precisa, a imagem capturada precisava ser de um rosto que estava olhando quase que diretamente para a câmera, com pouca variação de luz ou expressão facial da imagem no banco de dados. Isso era um grande problema.

Na maioria dos casos, as imagens não eram tiradas em um ambiente controlado. As menores alterações na luz ou na orientação poderiam reduzir a eficácia do sistema, de modo que não poderiam ser combinadas com nenhuma face do banco de dados, levando a uma alta taxa de falha.

Para solucionar esse problema surge um software de reconhecimento facial que usa um modelo 3D, que fornece mais precisão no processo. Capturando, em tempo real, uma imagem em 3D da superfície facial de uma pessoa, o reconhecimento facial 3D usa características distintas da face – onde o tecido rígido e o osso são mais aparentes, como as curvas da cavidade ocular, nariz e queixo – para identificar o sujeito. Essas áreas são únicas e não mudam com o tempo.

Usando profundidade e um eixo de medição que não é afetado pela iluminação, o reconhecimento 3D facial pode ser usado até mesmo no escuro e tem a capacidade de reconhecer uma pessoa em diferentes ângulos de visão, com o potencial de reconhecer até em 90 graus (perfil do rosto).

Usando o software 3D, o sistema passa por uma série de etapas para verificar a identidade de um indivíduo:

1. Detecção

A aquisição de uma imagem pode ser realizada digitalizando uma fotografia existente (2D) ou usando uma imagem de vídeo para obter uma imagem ao vivo de um indivíduo (3D).

2. Alinhamento

Depois de detectar um rosto, o sistema determina a posição, o tamanho e a pose da cabeça. Como afirmado anteriormente, o indivíduo tem o potencial de ser reconhecido até 90 graus, enquanto com 2D, a cabeça deve ser girada pelo menos 35 graus em direção à câmera.

3. Medição

O sistema mede as curvas do rosto em uma escala submilimétrica (ou micro-ondas) e cria um modelo.

4. Representação

O sistema traduz o modelo em um código único. Essa codificação dá a cada modelo um conjunto de números para representar as características no rosto de um indivíduo.

5. Coincidindo

Se a imagem for 3D e o banco de dados contiver imagens 3D, a correspondência será feita sem que nenhuma alteração seja feita na imagem. Contudo, há um desafio atualmente enfrentando nos bancos de dados que ainda estão com imagens 2D. O modelo 3D fornece um indivíduo vivo com movimentos variáveis, sendo comparado a uma imagem estável e plana. A nova tecnologia está enfrentando esse desafio. Quando uma imagem 3D é tirada, pontos diferentes (geralmente três) são identificados. Por exemplo, o exterior do olho, o

interior do olho e a ponta do nariz serão extraídos e medidos. Assim que essas medições estiverem prontas, um algoritmo (um procedimento passo a passo) será aplicado à imagem para convertê-la em uma imagem 2D. Após a conversão, o software irá comparar a imagem com as imagens 2D no banco de dados para encontrar uma correspondência em potencial.

Figura 6: Como funciona o reconhecimento facial (Bonsor e Johnson, 2001)

6. Verificação ou Identificação

Na verificação, uma imagem é correspondida a apenas uma imagem no banco de dados (1: 1). Por exemplo, uma imagem tirada de um sujeito pode ser correspondida a uma imagem no banco de dados de um sistema de imigração para verificar se o sujeito é quem ele diz ser. Caso a identificação seja o objetivo, a imagem será comparada a todas as imagens no banco de dados, resultando em uma pontuação para cada correspondência em potencial (1: N). Neste caso, pode-se pegar uma imagem e compará-la a um banco de dados de fotos para identificar quem é o sujeito.

A tecnologia de reconhecimento facial avança cada dia mais para aumentar a sua precisão e confiabilidade. Nesse sentido, a empresa Identix criou um novo produto para

auxiliar na precisão, um *software* que utiliza a biometria da pele, a singularidade da textura da pele, para produzir resultados ainda mais precisos.

O processo, chamado *Surface Texture Analysis*, funciona da mesma forma que o reconhecimento facial. Uma foto é tirada de um pedaço de pele, chamado de *skinprint*. Esse pedaço é então dividido em blocos menores. Usando algoritmos para transformar o pedaço em um espaço matemático mensurável, o sistema irá distinguir quaisquer linhas, poros e a textura real da pele. Ele pode identificar diferenças entre gêmeos idênticos, o que ainda não é possível usando apenas o software de reconhecimento facial. De acordo com o Identix, ao combinar o reconhecimento facial com a análise da textura da superfície, a precisão da identificação pode aumentar de 20 a 25% (Bonsor e Johnson, 2001).

Percebe-se que a tecnologia de reconhecimento facial está cada dia mais precisa. O Facebook, por exemplo, é capaz de reconhecer rostos com incríveis 97,25% de precisão (Alecrim, 2014). Conforme os custos dessa tecnologia vão diminuindo e a sua confiabilidade vai aumentando, as possibilidades de sua utilização vão aumentando exponencialmente, podendo ser utilizada em diversas áreas do conhecimento.

2.4.2. Aplicações na Segurança Pública

O reconhecimento facial – usando algoritmos para corresponder às características faciais de uma pessoa em fotos e vídeos – já é comum em muitos aspectos da vida contemporânea. Ele é usado para marcar pessoas em redes sociais, desbloquear celulares e consoles de videogames e focar fotografias de celulares, e em breve, poderá ser utilizado para realizar *check in* de voos através de uma foto tirada do próprio celular do usuário (Fala Brasil, 2017).

Voltado para a segurança pública, o reconhecimento facial tem várias possibilidades de utilização, algumas das quais já são experimentadas em alguns países, como o sistema utilizado pelo Departamento de Veículos Motorizados (DMV) de Nova York. Implementado em 2010 e atualizado em 2016, o sistema de reconhecimento facial de Nova York conecta-se ao banco de dados de fotos de identificação e informações de identidade registradas pelos escritórios do Departamento de Veículos Motorizados do estado (Bump, 2018).

Desde a atualização de 2016, o governo de Nova York alega que o *software* levou a mais de 4.000 detenções por fraude envolvendo criminosos que tentaram roubar as identidades dos residentes de Nova York listados no banco de dados do DMV (Bump, 2018).

De acordo com um comunicado de imprensa (Cuomo, 2017), quando uma licença, passaporte ou foto de identificação é tirada em um escritório do DMV de New York, ela é automaticamente inserida no software de reconhecimento facial. Se uma foto inserida no sistema não corresponder a uma única identidade, ou se coincidir com a foto de um criminoso de nome diferente, os investigadores do DMV são notificados.

Quando o membro da equipe da DMV clica na possível notificação de fraude, ele pode expandir para uma página que mostra uma comparação de identidade antiga e nova. O DMV pode, então, optar por investigar mais internamente ou por denunciar a possível fraude à polícia (Bump, 2018).

Além das fotos de identificação tiradas em vários DMVs de Nova York, o sistema recebe fotos e outras formas de identificação dos bancos de dados das policiais federais e estaduais (Bump, 2018).

Desde 2010, o sistema notificou os funcionários do DMV para 21.000 possíveis casos de fraude, sendo que 7.000 desses alertas vieram após a atualização de 2016 (Cuomo, 2017).

Outra forma de aplicação é apontada pela empresa NEC Corporation, informando que seu software de reconhecimento facial pode ser usado de duas maneiras, uma das quais é chamada de *Watchlisting*. Com esse recurso, investigadores, agentes da lei e guardas de segurança podem conectar o software da NEC a uma transmissão ao vivo da câmera de segurança ou carregar um vídeo na plataforma durante a reprodução. A empresa diz que seu software pode destacar e capturar rostos que passam na frente da câmera em tempo real, adicionando-os a uma lista de imagens faciais (Bump, 2018).

O segundo recurso da NEC permite que os usuários executem imagens faciais no sistema fazendo o *upload* delas ou selecionando-as a partir de imagens coletadas no modo *Watchlist* para ver se a imagem combina com fotos ou imagens de identificação em vários bancos de dados policiais (Bump, 2018).

Outra aplicação é destacada pela empresa FaceFirst, com sede em Los Angeles, que alega oferecer um software que pode confrontar imagens carregadas em sua plataforma por um policial com imagens de um banco de dados de reconhecimento facial e fotos de identificação. Assim, por exemplo, o policial pode tirar uma foto de seu celular de um suspeito no local da ocorrência e o aplicativo da empresa faz uma varredura automática no banco de dados para verificar se há alguma correspondência, fornecendo a resposta em segundos (Bump, 2018).

De acordo com o site da empresa, os policiais podem usar o FaceFirst enviando um banco de dados de imagens para o sistema. De seus telefones celulares, os policiais podem

adicionar fotos, imagens de identificação ou outras imagens faciais fazendo o *upload* delas no sistema, ou tirando a foto, no local, com o aplicativo. Quando um policial registra um suspeito no sistema, o policial que faz o *upload* da imagem será solicitado a adicionar informações, como um nome ou notas, que serão vinculadas à imagem, caso essa pessoa ainda não esteja no banco de dados (Bump, 2018).

Em um estudo de caso (Facefirst, 2013), a FaceFirst declara que o Sistema Automatizado de Informações da Justiça Regional (*Automated Regional Justice Information System* – ARJIS), baseado no Condado de San Diego, usa o FaceFirst. As agências parceiras da ARJIS, incluindo o Departamento de Polícia de San Diego, o FBI, a Agência de Combate às Drogas e outros, usam o sistema desde 2013.

Em seus primeiros quatro anos de trabalho com estes clientes, a FaceFirst afirma que seu software gerou um total de mais de 12.000 "ações policiais", como detenções ou questionamentos (Facefirst, 2013).

No Reino Unido a polícia de Gales do Sul utiliza a tecnologia de reconhecimento facial automatizado (*Automated Facial Recognition* – AFR) como ferramenta na prestação do serviço de segurança pública. Foi realizada uma avaliação em 2017 para recolher dados da aplicação da tecnologia AFR (Davies, Dawson e Innes, 2018).

Começou com a Final da UEFA Champions League de 2017, realizada em Cardiff, onde foi observada a utilização da tecnologia pelos policiais e analisados os dados gerados pelo sistema. A intenção era compreender como as equipes de policiais interagiam com o sistema e quais resultados eram possíveis alcançar, assim como os desafios enfrentados na utilização do sistema (Davies, Dawson e Innes, 2018).

Os policiais de Gales do Sul usaram AFR em dois modos. O "AFR *Locate*" utilizou transmissões ao vivo de câmeras do tipo CFTV, geralmente montadas em vans policiais identificadas, para comparar medidas detalhadas das características faciais das pessoas contra um banco de dados de imagens de custódia da polícia. Essas imagens eram de todos indivíduos considerados pessoas de interesse. Normalmente, esse banco de dados continha de 600 a 800 imagens (Davies, Dawson e Innes, 2018).

O outro modo, "AFR *Identify*", era bastante diferente. Nesse caso, as imagens de suspeitos não identificados de cenas de crimes do passado foram comparadas ao banco de dados de custódia da polícia. Este banco de dados é composto de aproximadamente 450.000 imagens (Davies, Dawson e Innes, 2018).

No geral, a avaliação concluiu que o sistema AFR permitiu que a polícia identificasse suspeitos que eles provavelmente não seriam capazes de detectar. Durante o período de 12

meses da pesquisa, mais de 100 detenções e acusações foram – pelo menos em parte – assistidas pela AFR (Davies, Dawson e Innes, 2018).

Nos últimos 14 meses, o Sistema AFR da polícia de Gales do Sul alcançou 800 correspondências positivas e mais de 450 prisões. Durante um teste realizado com sete voluntários em uma partida de rugby entre País de Gales x Itália pelo campeonato *Six Nations* em 2018, o sistema detectou estes indivíduos em mais de 76% das ocasiões em que passaram pelas câmeras. Mesmo com os voluntários utilizando vários estilos de caminhada, vestuários na cabeça, acessórios como óculos e chapéus, a taxa de alertas falsos foi de 1 em 2.251 rostos detectados. Ou seja, o sistema teve uma boa taxa de precisão combinado com uma baixa taxa de alertas falsos (South Wales Police, 2019).

Em Portugal o reconhecimento facial é utilizado pelo Laboratório da Polícia Científica na investigação criminal e para controle de cidadãos estrangeiros nos aeroportos (Capucho, 2018).

Na investigação criminal, por exemplo, quando se recebe uma pessoa na galeria, são tiradas fotografias e armazenadas em um banco de dados associadas com o sistema de impressões digitais. Futuramente se espera que seja possível buscar pessoas na base de dados a partir de imagens de suspeitos em câmeras de vigilância. Além disso, a tecnologia é utilizada na reconstituição craniofacial, onde a partir de um crânio limpo é verificada a compatibilidade entre o crânio e uma fotografia, sobrepondo-as e estudando a probabilidade de a pessoa da fotografia ser a do crânio. Isso é importante para identificar cadáveres e como complemento de análises de DNA (Diário de Notícias, 2018).

Verifica-se que os *softwares* de reconhecimento facial estão ganhando força no campo da segurança pública. Isso pode resolver o problema de policiais terem que vasculhar milhares de imagens e fotos de identidade para detectar fraudes e corresponder imagens suspeitas com identidades.

Softwares de reconhecimento facial podem ajudar as agências de segurança a reduzir o tempo de investigações, levando a prisões mais rápidas e, possivelmente, salvando mais vidas.

2.4.3. Na China

A China é a referência mundial quando se tenta imaginar uma cidade ou um país dominado pela tecnologia de vigilância através de sistemas CFTV e reconhecimento facial.

Com mais de 170 milhões de câmeras CFTV, e outras 400 milhões a serem instaladas, o país detém o maior e mais moderno sistema de vigilância do mundo (BBC News, 2017).

O sistema de câmeras da China é capaz de reconhecer o rosto das pessoas e imediatamente associar às informações registradas no banco de dados. Além disso, essa tecnologia consegue identificar o gênero, idade e a etnia. Também permite associar o rosto do cidadão a informações como o carro que utiliza, quem são seus parentes e com que pessoas esteve em contato (BBC News, 2017).

Segundo um representante da fabricante de câmeras Dahua Technology, os equipamentos são capazes de associar o rosto de uma pessoa à uma identidade e rastrear seus movimentos por uma semana, e assim, com câmeras suficientes, é possível identificar com quem as pessoas se encontram frequentemente (BBC News, 2017).

O correspondente da BBC John Sudworth testou o sistema de câmeras chinês na cidade de Guiyang, onde a polícia tem um vasto catalogo digital que contém a imagem de cada residente da cidade (Liu e Xiqing, 2017).

De comum acordo, a polícia inseriu a foto e os dados de Sudworth como se ele fosse um suspeito no sistema e lançou um alerta, então, o correspondente foi dar uma volta na cidade. Em apenas sete minutos ele já estava sendo abordado pela polícia (Liu e Xiqing, 2017).

Com isso, o governo pretende não apenas impedir os crimes que estão acontecendo no momento, mas também os prevenir.

De acordo com a polícia de Guiyang, as informações de cidadãos comuns só são coletadas quando eles precisarem de ajuda. Caso contrário, os dados não são coletados, apenas permanecem no banco de dados do sistema, os quais somente são utilizados quando é necessário, afirma a policial Xu Yan (Liu e Xiqing, 2017).

Na província de Jiangsu, no leste da China, o sistema de reconhecimento facial foi instalado nas estações de trem e, entre maio de 2017 e agosto de 2018, a polícia prendeu 137 fugitivos com a ajuda dessa tecnologia (China Daily, 2018).

O sistema alerta a polícia assim que um suspeito é reconhecido quando entra na estação. Em um determinado caso, houve um alerta de um fugitivo e a polícia o capturou 10 minutos após entrar na estação de trem de Changzhou (China Daily, 2018).

No condado de Fanxian, na província de Henan, um homem entrou em uma área residencial monitorada por câmeras de vídeo e imediatamente o alarme foi acionado em uma delegacia de polícia local. Graças à tecnologia de reconhecimento facial, o polícia concluiu

que havia uma probabilidade de 95% de que o homem identificado era o suspeito de um roubo de uma bicicleta elétrica. Em menos de duas horas a polícia o prendeu (Xinhua, 2018).

Em menos de um ano, o sistema equipado com a tecnologia de reconhecimento facial ajudou a polícia de Fanxian a localizar e prender 80 suspeitos, incluindo dois que estavam na lista de procurados nacionais por suspeita de cometer crimes violentos (Xinhua, 2018).

No ano passado, em Zhengzhou, os policiais chineses começaram a testar óculos equipados com um sistema de reconhecimento facial durante o patrulhamento das estações de trem. Esses óculos são capazes de identificar suspeitos de terem cometido crime. Em uma semana a polícia capturou sete pessoas procuradas em casos de maior repercussão e outros 26 que viajavam com identidades falsas (Observador, 2018).

Esses óculos de sol equipados com câmera são capazes de identificar os rostos das pessoas que passam pelo policial e cruzar informações com a base de dados da polícia. Em 100 milissegundos, o equipamento é capaz de pesquisar 10 mil pessoas no sistema e imediatamente emitir um alerta para um tablet, caso seja o indivíduo seja identificado como suspeito de um crime (Observador, 2018).

A vantagem desse modelo em relação as câmeras fixas é que, no caso das últimas, existe um tempo entre a sala de comando receber o alerta e comunicar os policias no local, que as vezes nem estão próximos do indivíduo identificado, e essa lacuna temporal pode ser suficiente para que o suspeito consiga se misturar à multidão e não ser mais identificado. No caso desse novo equipamento, o policial é alertado e imediatamente já pode decidir qual será a sua próxima ação (Observador, 2018).

Um dos casos mais surpreendentes ocorreu em abril de 2018, quando um homem chinês foi reconhecido e preso entre uma multidão de 60.000 pessoas, em um show da estrela pop Jacky Cheung, na cidade de Nanchang. O suspeito foi identificado pelas câmeras equipadas com a tecnologia de reconhecimento facial da polícia instaladas na entrada do show. O homem que era procurado por crimes econômicos ficou surpreso com a prisão, pois não acreditava que poderia ser identificado entre tamanha multidão (BBC News, 2018).

Em janeiro de 2019, deputados federais e senadores do Partido Social Liberal (PSL) foram à China conhecer o sistema de reconhecimento facial. A intenção dos parlamentares é apresentar um projeto de lei no início do ano legislativo de 2019 que definirá a obrigação da implantação de tecnologia de reconhecimento facial em locais públicos para auxiliar as forças de segurança pública no combate ao crime e captura de suspeitos (Rebello, 2019).

2.4.4. Casos reais

A tecnologia de reconhecimento facial agregada a um sistema de CFTV pode ter resultados promissores, como alguns já elencados no exemplo chinês. Ao redor do mundo há outros exemplos de sucesso que reforçam o argumento de implementação dessa ferramenta.

Em Londres, a tecnologia de reconhecimento facial está sendo testada e já apresentou bons resultados. A polícia realizou os testes durante os dias de 17 e 18 de dezembro de 2018, com foco no comércio de natal, a fim de tentar identificar criminosos procurados. O resultado foram quatro prisões, sendo que duas das pessoas eram procuradas pela polícia, e as outras duas foram chamadas "prisões proativas" – uma por uma suposta ameaça de estupro e outra por um suposto delito de drogas (Corum, 2019).

A proposta é realizar mais 10 testes nos próximos meses e ao final apresentar uma avaliação completa dos resultados. O teste é realizado da seguinte forma: câmeras são fixadas em postes ou instaladas em vans, e utilizam o *software* desenvolvido pela empresa japonesa NEC para realizar a leitura facial das pessoas que passam pelo local. Essa leitura é, então, comparada a um banco de dados de fotos da polícia. Quando o *software* aponta uma correlação entre o rosto do indivíduo com uma foto do banco de dados, ele solicita que os policiais observem mais de perto o rosto (Corum, 2019).

A polícia de Londres deixa claro que o sistema não é uma ferramenta autônoma de tomada de decisão. O sistema é projetado para separar "o joio do trigo", ou seja, ele filtra os rostos de potenciais suspeitos entre milhares que passam no local, para que, então, um avaliador humano decida quais devem ser investigados (Corum, 2019).

A Índia teve um resultado impressionante na utilização dessa tecnologia. Diferente do que inicialmente se imagina na utilização da tecnologia de reconhecimento facial, que é para capturar criminosos procurados, a polícia indiana utilizou a tecnologia para rastrear crianças desaparecidas. Em apenas quatro dias do lançamento do novo sistema na cidade de Nova Delhi, a polícia identificou cerca de 3.000 crianças desaparecidas (Cuthbertson, 2018).

A tecnologia foi utilizada em cerca de 45.000 crianças em toda cidade, onde foram reconhecidas 2.930 crianças como desaparecidas. A Índia tem quase 200 mil crianças desaparecidas e cerca de 90 mil em várias instituições de cuidado infantil, sendo humanamente impossível, ou altamente improvável, localizar crianças conferindo fotos manualmente e combiná-las com as crianças localizadas nas ruas(Cuthbertson, 2018).

No Brasil, essa tecnologia ainda é muito recente e está começando a ser implantada. No carnaval de 2019, a tecnologia de reconhecimento facial foi testada nas capitais do Rio de Janeiro e da Bahia e obteve resultados de sucesso.

No Rio de Janeiro/RJ, 28 câmeras foram instaladas no bairro de Copacabana, e nos dez primeiros dias de março, o programa ajudou na captura de oito pessoas que estavam com mandando de prisão ou apreensão em aberto, e ainda, na recuperação de três veículos roubados. A polícia militar do Rio de Janeiro pretende ampliar a utilização das câmeras com reconhecimento facial (Alves, 2019).

Em Salvador/BA, um homem foi preso após ser identificado pelas câmeras de reconhecimento facial instaladas nos 42 portais de acesso aos circuitos de carnaval da cidade. Ele estava com um mandando de prisão em aberto e era procurado pela polícia por suspeita de homicídio. Mesmo estando maquiado e fantasiado, as câmeras foram capazes de identificá-lo, e então, foi preso pelos policiais militares que realizam a revista pessoal dos foliões (Redação Correio, 2019).

São diversas as possibilidades de utilização da tecnologia de reconhecimento facial, tanto nos setores de segurança pública como nos mais diversos setores da sociedade. Com o avançar da tecnologia, que aumenta a sua eficácia e diminui os seus custos, a sua implantação parece ser uma tendência irreversível.

3. DIREITOS FUNDAMENTAIS RELACIONADOS AO TEMA

3.1. Direito à segurança

Como foi dito no capítulo 01 deste trabalho, o conceito de Estado está intimamente ligado ao conceito de segurança. Uma das principais razões do Estado, inclusive uma das bases sólidas de sua criação e desenvolvimento, é a garantia da segurança ao seu povo. Somente através da segurança, outros direitos podem ser garantidos.

Apesar do senso comum e da mídia apontar para um conceito de segurança onde se tenta evitar a violência urbana e o terrorismo, atualmente, entende-se a segurança de maneira muito mais ampla. Limitar a segurança ao receio de ser roubado ou de ter sua integridade física ameaçada é discriminatório, uma vez que se observa apenas o lado daqueles destinatários da segurança que pertencem a grupos sociais mais privilegiados, que tendem a ter esse tipo de preocupação com seu patrimônio e sua vida. Contudo, esse ponto de vista não aborda aqueles grupos mais sensíveis da sociedade que tendem a não se preocupar prioritariamente com patrimônio, mas com outros aspectos de satisfação de suas necessidades humanas, como o desemprego, falta de saneamento básico, doenças, má alimentação e etc (Lunardi, [s.d.]).

Dessa forma, a segurança deve ser entendida de forma mais abrangente, excluindo a visão geral “ordem x transgressores”, e evoluir para um conceito que envolva a garantia de todos os direitos. Com isso, tendo em vista os excluídos do acesso a recursos sociais que causam insegurança, o Estado tem que oferecer condições básicas para a efetiva proteção de todos os direitos fundamentais, incluindo os sociais e coletivos, com vistas a atender todos os cidadãos, titulares desses direitos (Sarlet, 2005; Sabadell, 2007; apud Lunardi, [s.d.]).

Nesse sentido, a segurança está ligada ao estado de bem-estar social. A segurança pelo bem-estar não é um direito especifico, ele engloba os direitos sociais em que a sua satisfação resulta como um aspecto de segurança para o indivíduo. Assim, a segurança é o objetivo, o processo e o efeito da satisfação das necessidades humanas (Lunardi, [s.d.]).

O direito à segurança é a forma do Estado proteger o cidadão, através de normas e ações estatais, contra atos e ameaças de particulares, e do próprio poder público, que visam violar os diversos direitos pessoais (Sarlet, 2007, apud Lunardi, [s.d.]). Ou seja, quando se pensa em segurança, se tem em mente a proteção de um outro direito que está sendo ameaçado/violado, como patrimônio, saúde, integridade física, privacidade, alimentação, etc. Garantir a segurança se trata de assegurar a satisfação de todos os outros direitos. Com

isso, o "direito à segurança", que compreende as leis e as políticas públicas destinadas a garantia da segurança, também pode ser entendido como as ações que visam garantir a "segurança dos direitos" (Baratta, 2000, p.3, apud Lunardi, [s.d.]).

No intuito de se abarcar todos esses direitos protegidos pelo conceito de segurança, sem a exclusão de grupos minoritários, alguns autores defendem o uso do conceito de "segurança humana", que compreende todas as ações voltadas a evitar inseguranças de grupos ou indivíduos, independentemente de qual seja a sua causa (Sorj, 2005, apud Lunardi, [s.d.]). Nesse sentido, a segurança é definida como o cenário em que um direito é garantido de forma permanente em um nível satisfatório (Lunardi, [s.d.]).

O conceito de segurança humana apresenta característica mais abrangente, envolvendo tanto o conceito de *safety (freedom from want)*, quanto de *security (freedom from fear)*. E ainda, apresenta as seguintes características fundamentais (Gouveia, 2018):

1) Universalidade: é uma preocupação universal, um valor que deve ser alcançado por todas as pessoas;
2) Interdependência: é um propósito que depende das ações individuais de cada país, contudo, ferir a segurança humana em algum local ou região, afeta o direito em termos globais;
3) Prevenção: é um propósito que é melhor alcançado através da prevenção, sendo a repressão um método menos eficiente;
4) Humanidade: o ser humano é o elemento central desse propósito, assim, todas as ações tomadas no intuito de sua consecução devem objetivar o bem maior ao indivíduo.

Por fim, importa ressaltar o conceito de Direito da Segurança, apresentado pelo professor Jorge Bacelar Gouveia (2018, p. 119): "sistema de normas e princípios jurídicos que definem a organização e o funcionamento das estruturas de segurança, estabelecendo os seus poderes e limites, com vista à proteção dos direitos e bens jurídicos fundamentais dos cidadãos e das comunidades políticas".

3.1.1. Direito à segurança em documentos internacionais

Desde a fundação do Estado, a segurança é uma preocupação do povo. Assim, esse direito não poderia ficar de fora dos principais tratados e convenções internacionais, que vinculam o cumprimento pelos signatários, Estados e Organismos Internacionais, através do Direito Internacional Público. São alguns destes documentos:

1. Declaração de Direitos da Virgínia, de 1776, artigo 1º: "que todos os homens são, por natureza, igualmente livres e independentes, e têm certos direitos inatos, dos quais, quando entram em estado de sociedade, não podem por qualquer acordo privar ou despojar seus pósteros e que são: o gozo da vida e da liberdade com os meios de adquirir e de possuir a propriedade e de buscar e obter felicidade e *segurança*";
2. Declaração dos Direitos do Homem e do Cidadão, de 1789, artigo 2º: "a finalidade de toda associação política é a conservação dos direitos naturais e imprescritíveis do homem. Esses direitos são a liberdade, a propriedade, a *segurança* e a resistência à opressão";
3. Declaração Universal dos Direitos Humanos (DUDH), ONU, 10 de dezembro de 1948, artigo 3º: "todo indivíduo tem direito à vida, à liberdade e à *segurança pessoal*";
4. Declaração Americana do Direitos e Deveres do Homem, de 1948, artigo 1º: "todo ser humano tem direito à vida, e a *segurança de sua pessoa*";
5. Convenção Europeia dos Direitos do Homem, de 1953, artigo 5º: "toda pessoa tem direito à liberdade e *segurança*";
6. Pacto Internacional dos Direitos Civis e Políticos, de 1966, artigo 9º, 1: "toda pessoa tem direito à liberdade e à *segurança pessoais* […]";
7. Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica), de 1969, artigo 7º: "toda pessoa tem direito à liberdade e à *segurança pessoais*";

Em todos esses documentos internacionais está previsto o direito à segurança. Percebe-se o valor dado a esse direito, pois na maioria dos documentos ele está listado, juntamente, com os direitos à vida e/ou à liberdade, colocando-os no mesmo patamar de importância.

3.1.2. Direito à segurança no Brasil

A Constituição da República Federativa do Brasil de 1988 (CRFB/88), ainda em seu preâmbulo, destaca a segurança como um dos valores supremos da sociedade, juntamente com a liberdade, a igualdade e outros direitos fundamentais.

Em seu artigo 5º, *caput*, inserido no título referente aos direitos fundamentais, a CRFB/88 estabelece a segurança como um desses direitos: "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à *segurança*

e à propriedade […]". Mais uma vez a segurança aparece ao lado de direitos importantíssimos como a vida, a liberdade e a igualdade, mostrando o seu valor perante a sociedade brasileira (Minuscoli e Almeida, 2016).

No artigo 6º, *caput*, a Constituição Brasileira afirma a segurança como um direito social, ou seja, ligado à ordem social: "São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a *segurança*, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição". Assim, verifica-se que a segurança é um dos propósitos do Estado que possibilita ao indivíduo a conquista de seus próprios objetivos (Souza, 2008, apud Minuscoli e de Almeida, 2016).

E ainda, em seu artigo 144º, *caput*, a Carta Magna trata mais especificamente da segurança pública: "A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio […]". Nesse sentido, define a segurança pública como um dever do Estado e responsabilidade de todos, estabelecendo um conceito democrático de segurança pública (Souza, 2008, apud Minuscoli e de Almeida, 2016).

Assim, a segurança pública se define como um direito fundamental que concede ao titular benefícios que materializam a garantia da liberdade, da dignidade da pessoa humana e da igualdade, estabelecendo um estado de proteção que proporciona ao indivíduo o gozo de todos os demais direitos individuais e coletivos (Fabretti, 2014, apud Minuscoli e de Almeida, 2016).

Em resumo, a segurança pública é um direito fundamental que garante o exercício de todos os outros direitos da legislação brasileira, assegura o exercício da cidadania, fortalece o Estado Democrático de Direito, mantendo um estado de ordem, proteção e relativa ausência de perigo ao cidadão, que o ajuda na recomposição de sua vida (Valente, 2012, apud Minuscoli e de Almeida, 2016).

3.1.3. Direito à segurança em Portugal

A Constituição da República Portuguesa (CRP), de 02 de abril de 1976, é a lei fundamental do país. Ela estabelece a base para a ordem jurídica de Portugal e é a lei superior na ordem hierárquico-formal do Direito Português.

A CRP é constituída de 296 artigos sistematizados em quatro partes, sendo antecedido e seguido por partes não numeradas, a saber:

– Princípios Fundamentais (arts. 1º a 11º);

– Parte I – Direitos e Deveres fundamentais (arts. 12º a 79º);

– Parte II – Organização Econômica (arts. 80º a 107º);

– Parte III – Organização do Poder Político (arts. 108º a 276º);

– Parte IV – Garantia e Revisão da Constituição (arts. 277º a 289º);

– Disposições Finais e Transitórias (arts. 290º a 296º).

Essa Constituição concede tanta importância à segurança que destaca esse valor em várias de suas disposições. De forma geral, cabe salientar exemplos de destaque ao longo da Constituição (Gouveia, 2018):

– No preâmbulo: ao se preocupar com a instauração de um Estado de Direito Democrático, após a Revolução de 25 de abril de 1974;

– No tópico "Princípios Fundamentais": a afirmação da segurança como uma tarefa fundamental do Estado à serviço dos indivíduos, da comunidade política e dos seus bens e direitos fundamentais;

– Parte I – Direitos e Deveres fundamentais: neste tópico, que é considerado a principal base de positivação dos direitos fundamentais, está previsto os direitos à liberdade e à segurança, bem como outros fundamentos a eles pertinentes;

– Parte III – Organização do Poder Político: define a estrutura do poder Estatal e traz as competências na área de segurança de cada um de seus elementos, tendo um título especial reservado para a Defesa Nacional;

– Parte IV – Garantia e Revisão da Constituição: mesmo que não seja voltado especificamente para segurança, existem dispositivos a ela pertinentes, referentes ao limite material e circunstancial da revisão constitucional;

– Disposições Finais e Transitórias: de forma restrita e pontual, destaca preocupação com a segurança na transição do período revolucionário para o período constitucional, referente à incriminação dos antigos agentes e responsáveis da PIDE/DGS.

Devido às inúmeras referências às matérias de segurança, o professor Jorge Bacelar Gouveia (2018, p. 185) nomeia a CRP como "Constituição da Segurança", que contêm as normas e princípios regulatórios e o exercício do poder público nas atividades de segurança.

3.1.3.1. Direito à segurança como um direito fundamental em Portugal

A Constituição da República Portuguesa define em seu artigo 27, nº 1, que "todos têm direto à liberdade e à segurança". Este é o artigo central no que se refere à introdução do

direito à segurança na CRP, pois traz de forma taxativa esse direito Este tópico é baseado no livro de Gouveia (2018).

Contudo, os números seguintes desse artigo se debruçam exclusivamente sobre o tema liberdade, em suas dimensões e exceções. Assim, apesar do art. 27 apresentar o direto à segurança, é necessário analisar a constituição como um todo para se estudar de forma mais robusta esse direito.

Alguns conceitos trazidos ao longo da CRP são essenciais para formar o conceito de direito à segurança, principalmente determinados direitos fundamentais como: "a reserva da vida privada" (art. 26º, nº 1, da CRP), que guarda a intimidade de intromissões externas; "a inviolabilidade do domicílio" (art. 34º da CRP), que traz a garantia de um espaço físico reservado à vida pessoal do indivíduo, livre da invasão do poder público e de entidades privadas; a "inviolabilidade das comunicações" (art. 34º, nºs 1 e 4, da CRP), que garante a proteção do teor ou do conhecimento das comunicações individuais do público externo; "a liberdade de reunião e de manifestação pacíficas" (art. 45º, nº 1, da CRP).

Dessa forma, o direito à segurança pode ser entendido a partir de outros direitos fundamentais, onde a observação desses direitos gera a obrigação de deveres de proteção a bens e direitos pessoais e patrimoniais. Isto é, direitos como à vida, à integridade pessoal ou à liberdade pessoal, ao mesmo tempo que são direitos fundamentais individuais, por outro lado, produzem o dever de que todos os outros indivíduos respeitem esses direitos, sejam públicos ou privados; direitos fundamentais produzem deveres fundamentais correspondentes, sendo que o direito à segurança garante o cumprimento desses deveres.

No Direito Constitucional Português, o direito à segurança encontra-se no grupo dos direitos, liberdades e garantias, e ainda, é considerado um direito fundamental. Isso traz duas consequências: como direito fundamental, está em um patamar de superioridade hierárquico-formal dentro da ordem constitucional; dentro do conjunto "direitos, liberdades e garantias", tem uma maior proteção jurídico-constitucional, por estar dentro de conjunto de limites matérias de revisão constitucional.

O titular do direito à segurança, como conta no art. 27º, nº 1, da CRP, são "Todos", não especificando, como acontece em outros artigos, se "pessoas", "cidadãos" ou "indivíduos", ou seja, é a forma mais ampla que se pode imaginar, cobrindo todas as pessoas, independente se estrangeiro ou nacional, de cidadania, ou de qualquer outro vínculo jurídico-político.

O objeto do direito à segurança, isto é, o bem jurídico protegido por esse direito fundamental, vai além da proteção da esfera pessoal ou patrimonial do indivíduo. O direito

à segurança visa proteger todos os outros direitos fundamentais (ou pelo menos a maioria deles) pelo titular, como a liberdade de locomoção, a reserva da vida privada, a liberdade de reunião e etc. Dessa forma, o direito à segurança adquire a função de "direito fundamental sobreposto", onde o seu objeto se torna a soma dos objetos específicos de cada um dos outros direitos fundamentais (Gouveia, 2018, p. 299).

Por fim, o direito à segurança possui tanto uma dimensão negativa quanto positiva. Na dimensão negativa, significa dizer que esse direito defende a esfera protegida do titular contra ofensas do poder público. Já na dimensão positiva, obriga o poder público a fornecer níveis de segurança através dos meios matérias e jurídicos possíveis (Gouveia, 2018).

3.2. Direito à privacidade

O tema privacidade está cada vez mais latente na atual sociedade tecnológica em que vivemos. Com a internet e as redes sociais, o mundo nunca teve tanta informação na palma da mão como se tem hoje. Podemos ter informações diárias do que está acontecendo na vida de nossos familiares e amigos, mesmo eles estando em outro continente.

Além disso, atualmente, os equipamentos tecnológicos estão cada dia mais avançados, e nos permitem gravar e tirar fotos com alcance e qualidade jamais vistas, mesmo nos nossos celulares. Aliado a isso, temos tecnologias de reconhecimento facial que constantemente nos marcam em fotos de amigos nas redes sociais, até mesmo sem o nosso consentimento. Estamos sendo vistos, analisados e "curtidos" constantemente, sem pararmos para pensar em que isso afeta a nossa privacidade.

Esse binômio, avanço tecnológico-privacidade andam juntos, e enquanto um cresce, o outro tende a se retrair. É sabido que não se pode frenar o avanço tecnológico, portanto é importante saber como lidar com a privacidade diante desse cenário de evolução. Esse capítulo irá abordar o tema privacidade, seus conceitos básicos, seu histórico, como sendo direito fundamental e demais aspectos pertinentes ao assunto.

3.2.1. Breve histórico do direito à privacidade

A palavra "privacidade" está relacionada com o termo "privado", que advém do termo em latim *privatus*, que por sua vez significa "separado de". O conceito de privacidade nasce na Antiguidade Clássica, onde a esfera pública (*polis*) se diferenciava da esfera privada (*oikos*) (Aristóteles, 2003, p. 30, apud Correia, 2014, p. 01). Enquanto a esfera pública se

referia à liberdade política dos cidadãos, a esfera privada estava relacionada à família, às questões econômicas e biológicas.

O conceito foi evoluindo e "privacidade" passou a fazer referência ao que é pessoal, quer seja no âmbito familiar, quer seja no círculo relacional de cada indivíduo (amigos). Além disso, o conceito se refere ao domínio protegido onde cada pessoa é livre para agir e decidir, independente das vontades e das influências da esfera pública, do Estado e da sociedade em geral. No Iluminismo, a proteção à privacidade se aproximou de sua definição atual (Correia, 2014). John Locke (2006, apud Correia, 2014), um dos principais pensadores da época, afirmava que o poder vinha das pessoas, os quais, desse modo, detinham do direito de se ver protegidos das intromissões do poder público.

Em 1791, nos Estados Unidos da América, foi promulgada a chamada *Bill of Rights* (Carta dos Direitos), que eram as dez primeiras Emendas à Constituição dos EUA. A quarta emenda garantiu ao povo americano o direito à inviolabilidade de suas pessoas, casas, papéis e posses contra busca e apreensão arbitrárias.

Foi a partir dessa quarta emenda que surgiu o primeiro estudo jurídico da história sobre a privacidade, o artigo *The Right to Privacy* (O Direito à Privacidade), escrito por Samuel D. Warren e Louis Brandeis, e publicado na *Havard Law Review*, em 1890, que consagrou esse direito como "*right to be let alone*"(o direito de ser deixado sozinho) (Gamiz, 2012).

Após a Segunda Guerra Mundial, a preocupação com os abusos contra os direitos humanos, e consequentemente contra a privacidade, se intensificou. Foi nesse cenário que a Organização das Nações Unidas (ONU) proclamou a Declaração Universal dos Direitos do Homem, em 1948, que em seu artigo 12 preconiza o direto à privacidade: "Ninguém será sujeito a interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques" (Gamiz, 2012).

No ano seguinte à promulgação da carta da ONU, foi publicado a obra "1984", do célebre escritor inglês George Orwell (2007), que, inspirado em experiências de países totalitários dos regimes nazistas e comunistas, advertia sobre uma sociedade totalmente vigiada, sem qualquer privacidade. A obra inspirou a criação do *reality show Big Brother* – mesmo nome do ditador do livro "1984", que no romance estampava cartazes por todos os lados com a frase "O Grande Irmão está observando você" – um programa televisivo que em que os participantes abdicam de sua privacidade e são vigiados vinte e quatro horas por dia (Gamiz, 2012).

Com o avanço tecnológico do séc. XX, a privacidade nunca esteve tão exposta. Câmeras fotográficas capazes de aproximar imagens muitas vezes, supercâmeras de vídeo, e principalmente a internet, que une informações de forma global, onde qualquer pessoa tem acesso à um mundo de informações sobre outro. Atualmente, tem se vivido um outro patamar de exposição advindo do desenvolvimento e proliferação das redes sociais no início do séc. XXI, que estimulam a auto exposição em troca de oportunidades comerciais ou, simplesmente, da sensação de bem-estar de ser admirado por outros desconhecidos.

A verdade é que quanto mais a tecnologia avança, mais o assunto privacidade vem à tona. O binômio tecnologia-privacidade anda junto, e quando se tenta fortalecer um dos lados, o outro lado protesta para não se ver extinto ou obsoleto. O desafio é promover o avanço tecnológico para o incremento da qualidade de vida sem ofender os direitos fundamentais do ser humano.

3.2.2. Direito à privacidade em documentos internacionais

Reforçando o cuidado com esse direito, outros documentos internacionais, que se seguiram após a Declaração Universal dos Direitos do Homem da ONU, reafirmaram o direito à privacidade. A seguir temos exemplos importantes:

1) Convenção Europeia de Salvaguarda dos Direitos do Homem e das Liberdades Fundamentais, Roma 1950, artigo 8.1: “toda a pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência”;
2) Pacto Internacional relativo aos direitos civis e políticos, ONU, 1966, artigo 17.1 e 2: “ninguém será objeto de intromissões arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio, ou na sua correspondência, nem de ataques ilegais à sua honra e à sua reputação. Toda a pessoa tem direito à proteção da lei contra tais intromissões ou tais atentados”;
3) Convenção Americana sobre os Direitos do Homem, São José, Costa Rica, 1969, artigo 11.2 e 3: “ninguém pode ser objeto de ingerências arbitrárias ou abusivas na sua vida privada, na vida da sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e à sua reputação. Toda a pessoa tem o direito à proteção da lei contra tais ingerências ou tais ataques”;
4) Convenção sobre os Direitos da Criança. ONU, 1990, artigo 16.1 e 2: “nenhuma criança será objeto de intromissões arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais

contra a sua honra e a sua reputação. A criança tem o direito à proteção da lei contra tais ingerências ou tais ataques";

5) Carta dos direitos fundamentais da União Europeia, Nice, 2000, artigo 7: "toda a pessoa tem o direito ao respeito da sua vida privada e familiar, do seu domicílio e das suas comunicações";
6) Convenção internacional sobre a proteção de todos os trabalhadores migrantes e dos membros da sua família, ONU, 2003, artigo 14: "nenhum trabalhador migrante ou membro da sua família será objeto de intromissões arbitrárias ou ilegais na sua vida privada";
7) Carta Árabe dos Direitos do Homem, Conselho da Liga dos Estados Árabes, Tunis, 2004, artigo 21 a, e b: "ninguém será objeto de intromissão arbitrária ou ilegal na sua vida privada, na sua família, no seu domicílio, ou na sua correspondência, nem de ataques à sua honra e à sua reputação. Toda a pessoa tem o direito à proteção da lei contra tal intromissão ou ataque";
8) Convenção sobre os direitos das pessoas deficientes, ONU, 1995, artigo 22: "nenhuma pessoa deficiente, seja qual for o seu lugar de residência ou o seu meio de vida, será objeto de intromissões arbitrárias ou ilegais na sua vida privada";
9) Convenção sobre os Direitos do Homem e a Biomedicina, 1997, artigo 10, parágrafo 1: "o seu direito ao respeito da sua vida privada tratando-se de informações referentes à saúde". E, no mesmo sentido, o Protocolo adicional à Convenção sobre a investigação biomédica, 2005, artigo 25, parágrafo 1: "toda a informação de caráter pessoal recolhida por ocasião de uma investigação médica é considerada confidencial, e é tratada no respeito pelas regras referentes à proteção da vida privada".

3.2.3. Privacidade no Brasil

Na legislação brasileira, o direito à privacidade foi estabelecido, genericamente, pela Constituição Federal de 1988, por meio do inciso X do artigo 5º, que diz: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

De acordo com os estudos de Sampaio (1998, p. 268) referentes a esse tema, o termo 'intimidade' advém do latim *intimus*, que significa "íntimo, mais recôndito, interior", relacionado, ainda, com a noção de confiança e segredo, como pode ser visto nos termos:

amici intimi (amigos íntimos), *intimus consilus* (confidentes de segredos) e *intima militia* (amizade íntima).

Ainda de acordo com o estudo de Sampaio, "privacidade" deriva do latim *privatus*, que significa "privado, particular, próprio, individual, pessoal". Dele derivam adjetivos como *private, privée, privatezza, privato* e privado – vida particular. Privacidade é um conceito mais amplo que intimidade, ele enquadra tudo aquilo que o indivíduo deseja que não se torne de conhecimento público.

Quando se refere ao uso dos termos no cotidiano, "ter intimidade" diz respeito a um terceiro que tem acesso a um espaço de reserva de um indivíduo. Assim, seria uma situação ou qualidade que se usufrui perante o outro: ser próximo o suficiente para lhe expressar sentimentos, emitir opiniões, ser confidente ou fazer algum tipo de pedido, sem formalidades. Dessa forma, "invadir a intimidade" implica em tomar conhecimento de segredos e assuntos pessoais de outro, estar em um âmbito restrito a poucos ou a ninguém (Sampaio, 1998, p. 269).

Já no termo "ter vida privada" há uma pequena diferença no sentido, pois se refere ao próprio titular da oração, e não uma qualidade que se possuiu em relação a outro. E mais, o significado também é distinto, pois expressa o sentido de ter vida própria, autônoma, independente. Quanto ao termo "invadir a vida privada", esse não difere tanto de "invadir a intimidade", ambos trazem uma noção de intrusão no espaço de autonomia ou de independência (Sampaio, 1998, p. 269).

A doutrina e jurisprudência brasileira, de forma geral, têm dificuldade na homogeneização da utilização dos termos referentes ao direito à privacidade. Além desse último, se utiliza termos como: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, além de outros menos utilizados como privatividade e privaticidade. A pluralidade de termos utilizados também na doutrina estrangeira certamente contribui para esse ambiente heterogêneo (Sampaio, 1998).

A dificuldade de se definir, categoricamente, os termos "privacidade" e "intimidade" na doutrina brasileira faz com que os operadores do direito, de modo geral, empreguem os dois termos indistintamente (Gamiz, 2012).

Mas essa dificuldade não está somente ligada a questões doutrinarias, e sim ao próprio sentido de intimidade e vida privada. É impossível definir, com caráter geral, tais conceitos, uma vez que seu sentido deve levar em conta o comportamento da pessoa analisada, juntamente com fatores externos, para então poder se chegar a uma conclusão sobre o âmbito concreto da vida privada e da intimidade de determinada pessoa (Pereira, 2003).

No Brasil, os autores costumam utilizar expressões como “direito à vida privada”, “direito à intimidade”, “direito ao resguardo”, “direito ao recato” e “direito ao segredo” como sinônimos. No entanto, ao se analisar o art. 5º da CRFB/88, verifica-se o amparo aos direitos à intimidade e à vida privada de forma distinta: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas…”. Apesar de existir muitos pensamentos na doutrina brasileira de que a intimidade é um segmento mais restrito da privacidade, a Constituição Brasileira fez distinção entre os institutos, consagrando expressamente a proteção de cada um deles.

Além disso, importa destacar que a CRFB/88 não assinala de forma expressa o termo privacidade. A verdade é que, até o início da década de 1990, essa palavra estava igualmente ausente de quase todos os dicionários brasileiros. Quando surgiu, trouxe também o sinônimo “privatividade”, e com isso, a polêmica: privacidade ou privatividade? Os que defendem a utilização desse último dizem que “privacidade” (derivada de *privacy*) é um anglicismo desnecessário (Silva Neto, 2001).

Apesar dessa discussão, a doutrina atual adota mais comumente a expressão privacidade. Esse termo parece a opção mais razoável, pois é especifico o suficiente para se diferenciar de outras expressões como imagem, honra ou identidade pessoal, bem como é claro o suficiente para especificar o seu conteúdo, resultado da sua atualidade. Tal escolha não deriva somente da fragilidade das demais opções, mas principalmente por unificar adequadamente os valores expressos pelos termos intimidade e vida privada (Doneda, 2006).

Ainda que não haja unanimidade sobre o assunto na doutrina brasileira, decorrente da complexidade do tema, muitos têm preferido utilizar a expressão “direito à privacidade” em sentido genérico e amplo, devido a sua abrangência terminológica e por poder englobar todas as manifestações da esfera íntima, da vida privada e da personalidade a que a CRFB/88 se refere.

3.2.3.1. Conceito de privacidade no Brasil

Uma das dificuldades para se entender o conceito de privacidade consiste no fato de que o instituto compreende vários aspectos, ou vários âmbitos de proteção, como a honra, a imagem, a intimidade e a vida privada. Com isso, quando há a violação de um desses direitos, não necessariamente ocorre a violação dos demais (Gamiz, 2012).

Outro obstáculo é precisar a extensão e o conteúdo desse direito, uma vez que o interesse é de caráter altamente subjetivo, variando de pessoa para pessoa. Os valores sociais

são diferentes e mutáveis de acordo com o tempo e o espaço, e o sentimento nuclear oscila de acordo com cada pessoa. Assim, fica evidente a dificuldade dos autores em estabelecer um conceito do direito à intimidade. A tarefa se torna mais difícil quando se deve determinar em que medida, ou em que situações, o direito à intimidade deve ser sacrificado em prol de um outro direito ou interesse juridicamente protegido, quando os dois se colocam em posição completamente antagônica (Silva, 2003).

Seria importante ter um conceito mínimo universal para o direito à privacidade, contudo, não é possível, a princípio, conceituar intimidade e vida privada em toda a sua extensão e plenitude. Seus limites exatos só podem ser medidos de acordo com o caso concreto (Sampaio, 1998).

Apesar da dificuldade apresentada em determinar o conceito de privacidade, é admissível concluir que ela sempre esteve diretamente vinculada ao estado da tecnologia em cada sociedade e época. É possível, inclusive, levantar a hipótese de que a construção de estruturas jurídicas e sociais que atuam na problemática da privacidade são respostas diretas a uma nova condição da informação, definida pela tecnologia (Doneda, 2006).

Dessa forma, o entendimento da privacidade deve levar em conta os fatores vigentes à época de sua aplicação, como lugar, espaço e meio. Esses fatores podem ser essenciais para se atingir um conceito de privacidade de maneira a resguardar uma pessoa que queira proteger aspectos íntimos de sua vida em relação à terceiros.

Todos temos uma noção do que é a nossa própria intimidade, mas quando se fala em definir o direito e precisar seu conteúdo, as dificuldades são insuperáveis (Silva, 2003). Assim, na tentativa de se definir um conceito a esse direito de contornos imprecisos, a doutrina brasileira tende a recorrer à jurisprudência como forma de entender o alcance desse direito (Araújo, 2000).

Diante da complexidade de se definir o direito à intimidade e à vida privada, e para não se ter um conceito demasiadamente vago e volátil, incapaz de ser utilizado, é importante definir premissas metodológicas, a fim de entender melhor o seu conceito. Essas premissas podem ser elencadas da seguinte forma (Sampaio, 1998):

1) São direitos invioláveis a intimidade e a vida privada e gozam de proteção constitucional formalmente transcrita no art. 5º, inc. X;
2) O direito à vida privada e à intimidade constituem estruturas formais de direito fundamental;
3) Devido ao fato de estarem ligadas à fatores pessoais e culturais, bem como, vinculadas à evolução tecnológica, a intimidade e a vida privada devem ser

> entendidas de forma aberta, dinâmica e flexível, de forma acompanhar essa constante evolução.

Ainda reforçando o argumento da dificuldade de se conceituar privacidade e intimidade, Pereira (2003) argumenta que não é apenas a conjuntura externa que influencia na definição do direito à intimidade, mas também a própria pessoa é um fator determinante no momento de se estabelecer o âmbito de sua intimidade. Cumpre ressaltar que é o próprio indivíduo que determina o seu âmbito íntimo, que deve ser respeitado pelos demais. De fato, algumas condicionantes materiais ou sociais podem influenciar no que se diz ser íntimo, mas no final, é sempre a pessoa que decide os limites de sua própria intimidade.

Assim, se torna impossível determinar um conceito geral de direito à intimidade, visto que os limites da intimidade se alteram de pessoa para pessoa, o alcance do direito também irá variar de uma pessoa para outra.

Em resumo, o conceito de direto à intimidade é condicionado pelas circunstâncias externas, mas não impedem que o próprio indivíduo escolha a extensão do seu domínio íntimo. Com isso, fica claro a complexidade de se definir, com precisão, o direito à intimidade, pois, de acordo com o exposto, o seu conceito é de geometria variável, sendo possível seu entendimento somente de acordo com o caso concreto.

Mesmo diante da dificuldade de se conceituar intimidade e privacidade, alguns autores brasileiros tentaram definir esses institutos. Para Bastos e Martins (1989, p. 63), a privacidade constitui a "… faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano".

Percebe-se o objetivo dessa definição de assumir um aspecto negativo de exclusão do referido direito, assim como um aspecto positivo de controlar o que deve ou não ser conhecido pelos demais. Esse raciocínio também é seguido por Jabur (2000, p. 254), que destaca como característica da privacidade a possibilidade de eliminar do conhecimento de terceiros fatos que o titular pretende preservar para si próprio.

Mesmo sabendo ser impossível definir privacidade e intimidade, Pereira (2003, p. 140) adota o seguinte conceito: "É o direito das pessoas de defender e preservar um âmbito íntimo, variável segundo o momento histórico impetrante, no qual estas possam desenvolver sua personalidade, bem como o poder de controlar suas informações pessoais, as quais, ainda que não formem parte da vida privada das mesmas, possam revelar aspectos de sua personalidade".

Esses conceitos nos ajudam a nortear um entendimento sobre o tema, mas os próprios autores reconhecem suas limitações. Isso se deve ao fato de que esse conceito é mutável e contextual, sendo que cada indivíduo pode, diferente dos demais e até de si próprio ao longo de sua vida, ter sua definição do que é íntimo ou privado, influenciado por aspectos culturais, políticos, religiosos, filosóficos e até climáticos, e inclusive por circunstâncias próprias ou de um dado momento existencial que pode permitir significados nunca cogitados (Sampaio, 1998).

Assim, a forma que pode ser considerada mais correta para se entender esse conceito é considerar os fatores que circundam cada caso concreto.

3.2.3.2. Privacidade: um direito fundamental

Os direitos fundamentais são previsões legais necessárias a todas as constituições, pois consagram o respeito à dignidade da pessoa, restringe o poder estatal e permite o pleno desenvolvimento da personalidade humana. Os direitos fundamentais podem ser definidos como o conjunto oficializado de direitos e garantias do ser humano que tem por objetivo básico o respeito a sua dignidade, através da sua proteção contra poder autoritário do Estado e a implementação de condições mínimas de vida e desenvolvimento da personalidade humana (Moraes, 2003).

Como o direito à privacidade é entendido como um direito fundamental, este foi inserido na CRFB/88, no Título “Dos Direitos e Garantias Fundamentais”, art. 5º, inc. X, onde prevê a inviolabilidade da intimidade e da vida privada.

O direito à privacidade é considerado como um direito fundamental de primeira geração, pois é um atributo inerente à individualidade da pessoa e tem a natureza de um Direito Negativo, ou seja, exige a abstenção do Estado, que é o seu principal destinatário (Gamiz, 2012).

A classificação dos direitos fundamentais em gerações é importante para hierarquiza-los, com o intuito de definir que direitos são mais relevantes do que outros e, quando confrontados, quais devem triunfar, de acordo com a análise de cada situação (Vieira, 2006).

Além disso, o direito da privacidade é considerado um direito da personalidade, ou seja, um direito essencial à pessoa humana e que possui a finalidade de preservar a sua dignidade (Aieta, 1999). Nesse sentido, o direito da privacidade possui características que o qualificam e o identificam como direito personalíssimo, quais sejam (Gamiz, 2012) :

1) Inato: ou originário, ele surge automaticamente com o nascimento com vida, ou seja, a partir do primeiro respiro pulmonar humano;
2) Vitalício, perene ou perpétuo: é um direito essencial, não pode faltar a nenhum ser humano. Está apto a ser usufruído a qualquer instante da vida, sendo perene (ou perpétuo), pois permanece com o indivíduo por toda sua vida;
3) Extrapatrimonial: não é possível estimar o seu valor, apesar de caber compensação pecuniária em casos de lesão ao direito;
4) Indispensável: não se pode renunciar, dispensar ou alienar o direito;
5) Imprescritível: o direito não se extingue pelo uso e nem é perdido se não for exercido durante certo tempo;
6) Oponíveis erga omnes – impropriedade do vocábulo "absoluto": são oponíveis contra todos (erga omnes), ou seja, impõe a toda coletividade o dever de respeitá-los. Contudo, dizer que é "absoluto" é impreciso, pois um direito pode ser vencido quando confrontado com outro direito de igual categoria ou graduação.

3.2.3.3. Espécies de privacidade

A privacidade pode ser de diferentes espécies e é classificada de acordo com seu âmbito de proteção, sendo eles: física, do domicílio, das comunicações (ou dos dados), decisional e informacional. Essa classificação descreve as situações em que a privacidade necessita de proteção jurídica, cabendo um breve comentário sobre cada uma delas (Vieira, 2007).

O direito à privacidade física objetiva impedir invasões não autorizadas no espaço do corpo da pessoa, como nos casos de testes forçados de droga, e do direito de estar só, como no crime de perseguição. A privacidade física pode estar relacionada a uma sensibilidade cultural, dignidade pessoal ou até timidez.

O direito à privacidade do domicílio – com previsão constitucional no art. 5º, inc. XI da CRFB/88 – se refere à proteção da privacidade dentro do espaço onde a pessoa reside, mesmo que temporariamente, ou exerce atribuições profissionais, conforme entendimento doutrinário. Seu objetivo é proteger os chamados "segredos domésticos" e a "inviolabilidade do lar", impedindo a entrada de estranhos em sua residência ou sua permanência, sem o consentimento do morador.

A terceira espécie se refere ao direito à privacidade das comunicações, que se encontra disposto no inc. XII do art. 5º da CRFB/88. Tem por objetivo resguardar a privacidade em

todos os tipos de comunicação, como correspondência, comunicações telegráficas, dados e comunicações telefônicas.

A quarta espécie, o direito à privacidade decisional, se refere ao direito de cada indivíduo de poder escolher o seu próprio destino, tomas suas próprias decisões, como a liberdade social de viver a sua própria sexualidade.

Por fim, o direito à privacidade informacional ou direito à autodeterminação da informática. O direito visa proteger a divulgação não autorizada de informações de um indivíduo que podem ser recolhidas e armazenadas em formato digital. Também existe a preocupação de como as informações da pessoa são adquiridas por terceiros, que muitas vezes ocorre por meios ilícitos.

3.2.3.4. Público x Privado

Importante questão quando se estuda a privacidade é o entendimento do que é público e o que é privado. Enquanto o primeiro é o espaço comum e visível, o segundo se caracteriza por um espaço particular da vida privada individual, que não deve ser do interesse público, e nem deve ser divulgado sem o consentimento do próprio indivíduo (Gamiz, 2012).

Parece simples a delimitação desses conceitos, mas os avanços tecnológicos do mundo contemporâneo, aliado a convivência social que tende a privilegiar os interesses da maioria, tornam cada dia mais tênue essa fronteira. Com isso, o direito à privacidade vem sendo ameaçado.

Nesse sentido, existe um conflito entre o interesse público e o direito à privacidade. A divulgação de informações de pessoas na esfera pública pode ser muito útil para dar transparência dos atos do Estado à comunidade, contudo, deve ser ponderado se aquela informação não é inerente à vida privada daquele cidadão. Dessa forma, aspectos da vida privada não podem ser publicitados sem que haja um motivo justo relevante.

Assim, o direito à privacidade deve sempre ser preservado, mesmo no espaço público, a não ser que haja um interesse coletivo suficientemente relevante para aquisição/divulgação de dados pessoais.

Desse modo, para se entender se algo pode ser considerado público ou privado, é necessário avaliar o grau de ostensividade da informação, ou seja, se é de necessário conhecimento geral ou de resguardo individual. É importante perceber que a privacidade é um valor público, uma vez que tem importância para toda a comunidade, pois ninguém quer ver sua intimidade atacada (Gamiz, 2012).

3.2.3.5. Âmbito de proteção

No que se refere ao âmbito de proteção do direito à privacidade, este também é difícil de mensurar. O âmbito de proteção de um direto compreende uma situação na vida real garantida por um dispositivo constitucional que aponta os bens assegurados e a sua extensão de proteção, sendo efetivada através da norma que institui o preceito (Vieira, 2007).

Nesse sentido, o âmbito de proteção do direito à privacidade, no direito brasileiro, inclui a intimidade, a vida privada, o domicílio, a correspondência, as comunicações e os dados pessoais de um indivíduo, assegurando que não haja intervenção de terceiros não autorizados.

Outro aspecto importante quanto ao âmbito de proteção é a sua extensão. Quando se fala no direito à privacidade, sua extensão é extremamente elástica e variável. Isso porque o tempo, o espaço e o titular do direito são fundamentais para se definir abrangência de proteção (Gamiz, 2012).

No que se refere ao tempo, verifica-se a enorme diferença de realidade entre os anos de 1989 e 2019, com uma diferença de 30 anos. Os avanços tecnológicos tornaram a vida privada muito mais acessível do que era a 30 anos atrás, principalmente com a internet. Portanto, com o passar dos anos, a abrangência de proteção do direito se altera com a necessidade de resguardar a privacidade individual.

Quanto ao espaço, percebe-se que condutas nocivas em uma comunidade podem não ser assim consideradas em outras, pois as sociedades são diversas e com costumes diferenciados. Assim, o que se entende como privado depende da visão de cada grupo social.

Por fim, o indivíduo deve ser considerado nessa equação. Quando se trata de uma pessoa pública ou um artista, o seu direito à privacidade é reduzido, e há mais tolerância ao se interpretar a ofensa ao direito, pois estão sujeitos à fiscalização popular, no primeiro caso, ou sua profissão exige constante exposição à mídia, no segundo caso (Moraes, 2006).

3.2.4. Privacidade em Portugal

3.2.4.1. Conceito de privacidade em Portugal

Em Portugal, também, existe a dificuldade de se definir o conceito de privacidade, não havendo um consenso entre os diversos autores (filósofos, politólogos, juristas, etc), bem como, existe uma variedade de terminologias para o conceito “direito à privacidade”. Por exemplo, na França, *droit à la vie privée*; nos Estados Unidos, *right of privacy*; na Itália,

diritto alla riservatezza; na Alemanha, a autodeterminação sobre informações de caráter pessoal foi reconhecida como um direito fundamental: *recht auf informationelle selbstbestimmung*. Em Portugal, assim como no Brasil, foi adotada a expressão "direito à privacidade" ou "direito à vida privada". Além dessa diversidade de expressões, existe a variedade de dimensões da experiência da privacidade, uma vez que o seu significado e suas regras evoluem historicamente e variam culturalmente, ou seja, o que se compreende por privacidade não é o mesmo em todas as regiões, em todos os níveis sociais, em todos os países, e em todas as épocas (Correia, 2014).

Outra questão que se deve levar em conta para se entender o conceito de privacidade é a correta distinção de "público" e "privado". Na sociedade moderna atual em que se vive, esses conceitos estão cada vez mais confusos, pois a sociedade tende a ver a política como um espaço para regulação da esfera privada e da vida doméstica (Correia, 2014).

Nesse sentido, alguns autores exemplificam essa atual mistura conceitual. Bilbao Ubillos (2006, apud Correia, 2014) percebe uma interpretação dilatada do conceito de poder público, que acaba por se expandir e alcançar atividades aparentemente privadas, que chegam a se submeter a limitações constitucionais. Silva Filho (2001, apud Correia, 2014) aponta que, no mundo moderno, a humanidade passou a se interessar cada vez mais por riqueza e pela economia, e ainda, o individualismo foi ficando mais forte, assim, a esfera pública passou a se preocupar com o âmbito privado. Já Daniel Sarmento (2006, apud Correia, 2014), acredita que, com o aparecimento do Estado Social, a intervenção do legislador na esfera privada se intensificou, com a promulgação de regras que limitam a autonomia privada das pessoas em favor dos interesses coletivos.

Dessa dificuldade de se diferenciar o público do privado, e dessa confusa fusão entre os dois, resulta a falta de uma definição central do conceito de "privacidade", que é bem ilustrado pelas palavras do jurista Mota Pinto (1993, p. 504, apud Correia, 2014, p. 03), que diz que definir privacidade "chega a raiar os limites do impossível". O conceito de privacidade é impreciso e sem coesão, em razão da dificuldade de se ter um conceito que deve ser indeterminado e, com isso, se mostra ineficiente, sendo um verdadeiro "conceito elástico" (Mota Pinto, 1993, apud Correia, 2014).

Quando se traz para o campo do direito, a tentativa de se definir privacidade resulta em igual insucesso. Apesar das inúmeras tentativas de definição filosófica, sociológica, política ou psicológica de privacidade, não parece ter sido possível encontrar um conceito minimamente preciso, indispensável para embasar um regime jurídico coeso (Mota Pinto, 1993, apud Correia, 2014).

Apesar de admitir a dificuldade de se chegar a um conceito fechado de "privacidade", Mota Pinto (1993, pp. 508-509, apud Correia, 2014, p. 04) arrisca defini-lo da seguinte forma: "(...) por um lado, o interesse do indivíduo na sua privacidade, isto é, em subtrair-se à atenção dos outros, em impedir o acesso a si próprio ou em obstar à tomada de conhecimento ou à divulgação de informação pessoal (interesses estes que, resumindo, poderíamos dizer serem os interesses em evitar a intromissão dos outros na esfera privada e em impedir a revelação de informação pertencente a essa esfera); por outro lado, contrapondo-se fundamentalmente ao interesse em conhecer e em divulgar informação, e ao interesse em ter acesso ou controlar os movimentos do indivíduo". Essa tentativa de definição demonstra a problemática da proteção jurídica do direito à privacidade, uma vez que é repleta de conceitos genéricos e sem um núcleo central.

Ainda que seja difícil definir o conceito de "privacidade", o seu estudo traz alguns aspectos fundamentais desse conceito, como: informação (proteção de dados); comunicação (inviolabilidade da correspondência postal, informática, e de telefonemas); privacidade territorial (proteção contra a invasão do lar, do escritório, do atelier, etc.); e intimidade corporal. Para ser mais preciso, tem relação com questões da vida privada, como: a anatomia ou a intimidade, as origens sociais e familiares, a imagem física, corporal, a voz, os tempos livres de cada pessoa, seus hábitos de consumo, o estado de saúde, a correspondência epistolar e eletrônica, os amigos, a vida familiar, a situação patrimonial, a vida sentimental e sexual, os aspetos sigilosos pessoais ligados à sua profissão, a situação fiscal e bancária, o salário, as convicções políticas, e suas crenças religiosas (Correia, 2014).

Assim, a privacidade não está limitada somente à residência familiar, mas também em outros ambientes, mesmo que públicos, como igrejas, espaços de lazer, locais de trabalho, e até mesmo praças e ruas; isto é, sendo um assunto de natureza privada, este deve ser respeitado como tal em qualquer lugar, seja em local público ou privado (Correia, 2014).

Em resumo, a privacidade se trata de todas as informações sobre a pessoa, que ela pode escolher manter sob seu exclusivo domínio ou expor, escolhendo a quem, como quando e onde expor tal informação.

Dessa forma, a privacidade se trata de proteção de dados, que estão ligados com convicções pessoais e sentimentos, desde que não prejudiquem a sociedade, da possibilidade de ser deixado em paz e até de se manter anônimo. Em relação ao "direito à privacidade", este se trata da liberdade reconhecida juridicamente pelo Estado que cada pessoa tem seu espaço particular em relação a comunidade, protegido legalmente a níveis nacional e internacional (Correia, 2014).

Atualmente, tem surgido novos conceitos jurídicos sobre o tema, como o "direito à proteção de dados" e o "direito à autodeterminação informativa". Alguns autores defendem que esses conceitos são distintos do direito à privacidade (Olga, 1985, apud Correia, 2014). Contudo, as definições de "proteção de dados", ou de "autodeterminação informativa", nada mais são do que uma nova forma de aplicar o direito à privacidade, pois quando uma pessoa alcança qualquer um desses direitos, no fundo ela alcança uma parte do direito que está incluída no direito à privacidade. Com isso, entende-se que esses novos conceitos estão incluídos no direito à privacidade (Correia, 2014).

3.2.4.2. O direito à privacidade em Portugal

Em Portugal, a Constituição da República Portuguesa institui o direito à privacidade como um direito fundamental em seu art. 26º, nº 1: "a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar".

O direito à privacidade no direito português, assim como no brasileiro, compõe os direitos de personalidade, que são tidos como direitos absolutos, pois se estabelecem como uma obrigação passiva universal e impõem o dever de respeito por todos (Correia, 2014).

Se trata de um *ius in se ipsum*, um direito fundamental em que o bem a ser protegido é o próprio individuo, pois defende a sua necessidade inerente de autodeterminação. Somente direitos ilimitados e ilimitáveis, como os direitos de personalidade, são capazes de proteger o indivíduo dos riscos de violação existentes na sociedade moderna (Carvalho, 1981, apud Correia, 2014).

Para além da proteção constitucional e da condição de direito de personalidade, o Código Civil português prevê tutela ao direito à privacidade, em seu artigo 80 (Direito à reserva sobre a intimidade da vida privada): "todos devem guardar reserva quanto à intimidade da vida privada de outrem. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas".

Além disso, o artigo 483 do Código Civil declara o dever de indenizar a violação de direito alheio, sendo o direito de personalidade um desses direitos. Além da indenização pela responsabilidade civil, "a pessoa ameaçada ou ofendida pode requerer as providências judiciais adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça

ou atenuar os efeitos da ofensa já cometida", conforme prescreve o artigo 70, nº. 2, do mesmo diploma legal.

No âmbito do direito penal português, adota-se a doutrina das três esferas, onde devem ser diferenciadas as esferas da intimidade, a esfera da privacidade e a esfera da vida normal da relação (Carvalho, 1981, apud Correia, 2014).

O crime de devassa da vida privada está previsto no artigo 192 do Código Penal português, que pune "quem sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual; interceptar, gravar, registrar, utilizar, transmitir ou divulgar conversa ou comunicação telefônica; captar, fotografar, filmar, registrar ou divulgar imagem das pessoas ou de objetos ou espaços íntimos; observar ou escutar às ocultas pessoas que se encontrem em lugar privado; divulgar fatos relativos à vida privada ou a doença grave de outra pessoa".

Esse é um crime comum, ou seja, não depende da qualidade especifica da pessoa. Não se confunde com o crime de violação do sigilo profissional, previsto no artigo 195 do Código Penal, que se concretiza quando o autor é obrigado a observar o sigilo profissional (sigilo médico, judicial, bancário, etc). Dessa forma, o direito penal português reforça que a vida privada deve ser protegida, independentemente de o fato afetar a honra ou não. Nesse caso, o bem jurídico tutelado é a privacidade, e não a honra. Apesar disso, Código Penal tem a intenção não somente de impedir o acesso à informação (alíneas 'a', 'b' e 'c'), mas também a sua divulgação (alínea 'd') (Correia, 2014).

Por fim, o Código do Trabalho também promove a proteção aos direitos de personalidade ao dedicar uma subseção ao tema (artigos 14 a 22). O artigo 16 estabelece o direito à reserva da intimidade da vida privada: "O empregador e o trabalhador devem respeitar os direitos de personalidade da contraparte, cabendo-lhe designadamente guardar reserva quanto à intimidade da vida privada. O direito à reserva da intimidade da vida privada abrange quer o acesso, quer a divulgação de aspetos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afetiva e sexual, com o estado de saúde e com as convicções políticas e religiosas".

3.3. Conflitos enfrentados no direito à privacidade

Como foi demonstrado, tanto no Brasil como em Portugal, a privacidade é um direito fundamental e faz parte do rol de diretos de personalidade, ou seja, sua proteção é

absolutamente necessária para o desenvolvimento do ser humano como pessoa. Este tópico é baseado no artigo escrito por Correia (2014).

Contudo, mesmo estando sob tutela constitucional, nem sempre os tribunais condenam àqueles que, em tese, invadiram a privacidade de outrem. Por exemplo, em um caso que um jornalista fotografa uma figura pública na sua intimidade, nem sempre o fotógrafo será declarado culpado, algumas vezes a figura pública será indenizada, e em outras, o fotógrafo será absolvido. Isso porque, nesse caso, o jornalista invoca o seu direito de difundir informação verdadeira de interesse público através da liberdade de imprensa.

Verifica-se, aqui, um conflito entre dois direitos importantes: o direito à privacidade e o direito à informação. De acordo com cada caso, vão existir momentos em que o direito à informação se impõe ao direito à privacidade, e em outros momentos, o direito à privacidade se impõe ao direito de informação.

Uma vez que não existe hierarquia quando se confrontam dois direitos fundamentais, é complexa a análise de qual direito deve se sobrepor a outro. Neste exemplo, deve ser analisado se a informação de fato é de interesse público. Porém, essa não é uma análise simples, pois o conceito de "interesse público" é subjetivo e depende da cultura, do país, da região, do público, do jornalista, do magistrado, da época e etc. Assim, os tribunais têm um desafio enorme quando se trata do conflito desses direitos fundamentais.

Quanto ao conceito de privacidade, como já foi referido, também é de complexa interpretação, pois depende da cultura, do país, do indivíduo, da época e etc. A forma como se encara a privacidade pode mudar completamente de acordo com a região do planeta. Existem povos e culturas em que o conceito de vida privada é completamente distinto daquilo que se entende no Ocidente, onde a privacidade não é vista como uma necessidade fundamental, ou não é dada tanta importância a ela, ou onde o Estado tem um controle maior das liberdades individuais de seu povo. Por exemplo, nas ilhas Samoa, muitas casas não têm paredes e as atividades familiares podem ser vistas por todos do lado de fora.

Outros conflitos que existem, no que se refere ao direito à privacidade, são alguns ligados à identidade cultural de determinadas pessoas, como o Candomblé (religião oriunda do animismo africano), quando estes estão inseridos em uma sociedade distinta da sua originária, como é o caso de refugiados em países de cultura diferente. Algumas práticas dessa religião podem ser limitadas, ou até proibidas, mesmo que façam parte da identidade cultural e do direito à privacidade (associado à liberdade religiosa).

Nesse caso, há um conflito entre a liberdade de consciência religiosa, a identidade cultural, o direito à privacidade e o bem-estar social. Determinados rituais religiosos de

sacrifício, doutrinas que difundem a discriminação e o ódio, a não permissão de transfusões de sangue, a prática de suicídios coletivos, a exploração econômica por parte de seitas religiosas, etc., devem ser proibidos, mesmo que pertençam às íntimas convicções religiosas da pessoas, e que estas convicções estejam protegidas pelo direito à privacidade. Portanto, o direito à privacidade não é absoluto.

As diferentes formas de interpretação da privacidade não mudam apenas de acordo com os povos e culturas, mas também entre cada pessoa, mesmo que seja do mesmo país. Mesmo sendo um direito fundamental na cultura Ocidental, o que pode ser considerado como uma afronta à privacidade é altamente relativo e subjetivo, podendo ser diferente entre vários indivíduos. O que uma pessoa acredita ser uma transgressão a sua privacidade, outro irá considerar inofensivo. O direito à privacidade é guiado por uma série de limites, e a sua tutela recorre a um equilíbrio entre outros direitos, sendo assim, não se trata de um direito absoluto sobre os demais.

A própria Convenção Europeia dos Direitos do Homem cita algumas restrições e ingerências que podem ser impostas ao direito à privacidade por parte das autoridades públicas, em seu artigo 8, parágrafo 2: “desde que essa ingerência esteja prevista pela Lei e constitua uma medida que, numa sociedade democrática, seja necessária à segurança nacional, à segurança pública, ao bem estar económico do país, à defesa da ordem e à prevenção das infrações penais, à proteção da saúde ou da moral, ou à proteção dos direitos e das liberdades de terceiros”.

Dessa forma, com o intuito de proteger a segurança dos cidadãos, as autoridades podem não observar o direito à privacidade de certas pessoas, e assim, efetuar escutas telefônicas, consultar seus dados pessoais, ler suas correspondências, gravar conversas e etc., desde que esteja provado que essas ações sejam, de fato, necessárias.

Em casos de combate à corrupção, as autoridades podem desrespeitar o direito à privacidade e quebrar o sigilo bancário, e por razões de higiene, relativos ao direito à saúde pública, podem entrar em espaços privados de restaurantes. Em relação ao direito de conhecer as suas origens, por vezes reivindicado por um filho, pode ferir o direito à privacidade de um pai que não quer revelar o seu nome. Existe também o direito à história, que pode limitar o direito à privacidade de figuras históricas ainda vivas e revelar a sua descendência, em nome da investigação acadêmica e do interesse público.

E ainda, como já foi citado, em nome da liberdade de imprensa e do direito à informação, os jornalistas se intrometem na vida privada de figuras públicas, reivindicando que seus leitores têm direito a informações de interesse público sobre aquelas pessoas. A

liberdade de expressão, o direito do público à informação e a liberdade de imprensa, em algumas circunstâncias, impõe limites ao direito à privacidade. Quando uma pessoa exerce uma função pública, ou quando adquiri certa notoriedade, certos elementos da sua vida privada se tornam de interesse público, e assim, nesses casos, é difícil classificar como intromissão à privacidade a divulgação de certas informações.

Apesar de sua importância social, o direito à privacidade não é um direito absoluto, e deve encontrar equilíbrio entre os demais direitos, nesse último caso, o direito à privacidade e o direito à informação, que são ambos defendidos pela Declaração dos Direitos do Homem, por outras declarações e documentos internacionais, pela Constituição de alguns países – como a brasileira e a portuguesa –, e por outras leis vigentes. Nesse conflito de direitos, os tribunais têm fundamental importância, pois irão decidir, de acordo com o caso concreto, qual direito deve ser considerado mais relevante e se sobrepor ao outro (Correia, 2014).

3.4. A importância da privacidade como direito

A privacidade é um direito essencial para o desenvolvimento da personalidade de cada indivíduo. Para não se perder o foco da defesa desse direito, é importante ressaltar o seu valor. Este tópico é baseado no artigo escrito por Correia (2014).

De fato, a esfera da vida privada é algo essencial. Biologicamente falando, o ser humano, assim como outros animais, tem a tendência de demarcar o seu próprio território. Do ponto de vista psicológico, a privacidade é o que distingue a realidade externa da realidade interna, e é a base para afirmação da personalidade. Se o indivíduo fosse obrigado a viver constantemente sob os olhos do espaço público, ele acabaria por perder suas características de personalidade e se dissolveria no anonimato e no coletivo, como um produto da massa.

A privacidade é um espaço necessário para o desenvolvimento da personalidade. Dessa forma, o indivíduo não fica submetido ao controle social, que iria anular a sua dignidade, inviabilizar seu livre desenvolvimento psicológico e cercear a sua autonomia privada. Portanto, a privacidade não é apenas um escudo contra o exterior, mas um elemento positivo do desenvolvimento humano (Doneda, 2008, apud Correia, 2014).

A privacidade é fundamental para o exercício de direitos básicos, que estão vinculados ao conceito de pessoas livres e iguais, e de uma concepção democrática de privacidade (Lever, 2011, apud Correia, 2014). A privacidade é essencial para uma participação

democrática dos cidadãos no processo eleitoral, onde o voto é secreto e confidencial, só assim é possível o cidadão agir de forma livre, sem se sentir coagido social e politicamente.

No âmbito político, o direito à privacidade protege a democracia. Isso se prova quando os regimes ditatoriais e totalitários têm a tendência de acabar a privacidade individual dos cidadãos, como bem ilustra a celebre obra "1984", de George Orwell (2007).

A privacidade preserva a diferença entre as pessoas. Através da privacidade, os indivíduos desenvolvem a sua consciência e seus sentimentos, podendo levar a vida que consideram correta, sem entrar em confronto com os demais. Sem a proteção do direito à privacidade, é mais difícil garantir as diferenças morais, políticas, religiosas, etc., essenciais para o bom desenvolvimento da democracia.

É comum se utilizar o argumento do "não ter nada a esconder" ou do "quem não deve não teme" para defender a limitação da privacidade ou contestar a reivindicação desse direito. Contudo, esse argumento se apresenta mais complexo do que simplesmente "não ter nada a esconder". Esse argumento põe na balança dois lados que não têm o mesmo peso: cidadão x Estado; empregado x empregador; consumidor x comerciante; fraco x forte. Existe um lado que pode mudar as regras do jogo unilateralmente, que pode te considerar um bom ou mau cliente, uma boa pessoa ou uma ameaça, um bom ou mal empregado, com base nas informações que dispõem, podendo ser até falsas informações, ou informações pessoais que não se sabe que o outro lado possui. A relação apresentada na afirmação "não tenho nada a esconder, pois não transgrido as regras" é sempre desequilibrada. Não se espera somente do Governo que se respeite a privacidade, mas de todos que exercer poder sobre as pessoas, como empregadores, concorrentes, etc. É importante, para as pessoas, não deixar na mão das organizações com as quais se relacionam o poder de gerir as regras que regem suas vidas (Solove, 2010, apud Correia, 2014).

Para se entender o problema apresentado, Solove (2010, apud Correia, 2014) sugere a utilização da metáfora do livro "O Processo", de Franz Kafka (2009), que retrata como uma burocracia usa informações sobre as pessoas para tomar decisões a seu respeito, sem que a pessoa entenda como a informação é utilizada. Segundo o autor, a problemática apresentada pela metáfora de Kafka é mais relativa ao processo de tratamento das informações e a análise dos dados, do que com a sua recolha. A vigilância dos dados em si não é o problema, mas a impotência e a vulnerabilidade gerada pela utilização de informações sobre a pessoa, sem que ela possa entender e participar do processo, ou tomar conhecimento de quais dados a seu respeito estão utilizando. O resultado disso é o mesmo encontrado nas burocracias: erros, abusos, indiferenças, frustrações, falta de responsabilização e transparência. Tal tratamento

de dados influencia na relação dos indivíduos com as instituições do Estado, onde não só cria um sentimento de impotência e frustração, como também afeta toda estrutura social, ao mudar as relações das pessoas com as instituições que tomam decisões importantes sobre suas vidas.

De fato, pode acontecer que as pessoas que possuem os dados sobre os cidadãos interpretem esses dados de forma distinta, que não corresponde aos fatos reais, ou aplique regras diferentes para análise dos dados. Não se pode ter certeza de quem e como se aplicam as regras sobre os dados, por isso há a necessidade de proteger os dados pessoais. Um dos grandes problemas gerados pela utilização abusiva dos dados pessoais não é somente a restrição de certas liberdades, mas sim o desmoronamento da confiança social e a inibição generalizada na sociedade, que deixará de criar, opinar, criticar, agradar, desagradar, etc., com medo de que, aqueles que forem analisar seus dados, possam condená-lo.

O argumento de "nada a esconder" se fundamenta em uma visão de que a privacidade individual está em conflito com o bem comum ou algum tipo de interesse social. Contudo, os interesses de um indivíduo e da sociedade não são necessariamente desiguais. A proteção e o respeito pelo indivíduo e as liberdades civis formam a base de um elo social, uma estrutura de confiança que permite o funcionamento de uma sociedade. Assim, a privacidade tem sua importância social, mesmo protegendo a pessoa, o faz para o bem de toda sociedade (Solove, 2010, apud Correia, 2014).

Para a grande maioria dos indivíduos, as suas atividades da vida privada não são nem ilegais e nem embaraçosas, assim, a defesa da privacidade não se trata necessariamente de esconder coisas inconfessáveis, mas pode ser apenas o exercício do direito de limitar o acesso a informações pessoais. O problema dos programas de vigilância está no fato dos indivíduos não saberem, exatamente, quais dados são utilizados, de que maneira e com que finalidade.

Como demonstrado por Kafka (2009), o problema não está na vigilância dos dados em si, mas, principalmente, na vulnerabilidade e na impotência gerada por um tratamento de dados que exclui do processo o indivíduo analisado. Essa situação cria um desequilíbrio entre as pessoas analisadas e as entidades e instituições que recolhem e tratam esses dados, sobretudo quando, por exemplo, existe a reutilização dos dados para uma finalidade distinta daquela para o qual foram coletados, sem o consentimento ou ciência das pessoas. Isso acaba por fragilizar a democracia, em uma relação de forças desiguais (Solove, 2010, apud Correia, 2014).

Deste modo, a privacidade não deve ser encarada somente como um direito individual, mas também pela sua importância para a sociedade como um todo. Assim, o direito à privacidade vai além de sua importância para o desenvolvimento individual, e alcança o patamar de assegurar o bem-estar social. Sem a proteção do direito à privacidade, muitos outros direitos ficam fragilizados, como a liberdade pessoal e a igualdade de direitos. É importante se ter uma visão democrática da privacidade, onde o direito à privacidade seja coeso com esses direitos.

Consequentemente, a privacidade tem sua relevância na esfera política. Se por um lado, o direito à privacidade é importante para a democracia, por outro lado, a democracia é essencial para o respeito ao direito à privacidade. Somente através desse entendimento é que se alcança a ideia de que, perante outros direitos como a liberdade e a igualdade, o direito à privacidade assume um papel de algo necessário para garantir que esses direitos são, de fato, democráticos (Correia, 2014).

3.5. Proteção de Dados Pessoais em Portugal

A proteção de dados pessoais deriva diretamente do direito à privacidade, ou da proteção desse direito. O dado pessoal é toda informação relativa a uma pessoa singular identificada ou identificável (titular dos dados), como o nome, número de identificação, dados físicos, fisiológicos, genéticos, econômicos e etc[1]. Ou seja, ter o direito a proteção desses dados é pôr em prática a proteção do direito à privacidade, a fim de que pessoas não autorizadas pelo titular tenham acesso a esses dados, podendo causar danos de qualquer espécie ao titular ou à coletividade.

Na atual sociedade da informação tecnológica em que se vive, o dado pessoal é um produto que gera valor para as pequenas e grandes corporações. Assim, vários órgãos e empresas possuem dados pessoais para os mais diversos objetivos, desde dados sobre sua saúde, que auxiliam em diagnósticos médicos; até dados sobre seu perfil e suas preferências pessoais, para buscar seu par romântico ideal.

E tantos dados pessoais espalhados por diversas empresas e pela internet, nas mãos erradas, poderiam ser usados contra os titulares, ou outrem, para causar algum dano ou

[1] Art. 4º, 1 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – Regulamento Geral de Proteção de Dados – RGPD (*General Data Protection Regulation* – GDPR).

executar alguma fraude. Um caso recente que abalou o mundo da proteção de dados pessoais e da privacidade foi o escândalo Facebook-Cambridge Analytica. Nesse caso, informações de mais de 50 milhões de usuários do Facebook foram utilizadas, sem o consentimento dos titulares, pela empresa americana Cambridge Analytica para fazer propaganda política nas eleições americanas de 2016 (BBC, 2018).

É no contexto de garantir o direito à proteção dos dados pessoais, e em consequência, o direito à privacidade, que surgem as legislações sobre o assunto em todo mundo.

3.5.1. Evolução histórica da legislação

Desde 1976, a Constituição da República Portuguesa consagra a proteção dos dados pessoais, referente a utilização da internet, como um direito fundamental em seu artigo 35º (CNPD, 2019).

Contudo, somente quinze anos depois, foi aprovada a primeira lei de proteção de dados (Lei nº 10/91), que regulamentou a utilização e o controle dos dados pessoais e previu a criação da Comissão Nacional de Proteção de Dados Pessoais Informatizados – CNPDI, tendo sofrido alterações com a Lei nº 28/94.

Em 1995, foi publicada a Diretiva 95/46/CE do Parlamento e do Conselho, de 24 de outubro, relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Em 1997, na 4ª revisão constitucional da CRP, e a fim de se transpor adequadamente a Diretiva de Proteção de Dados de 1995, houve algumas alterações no artigo 35º, que consagrou constitucionalmente a existência de uma entidade administrativa independente para regular a proteção de dados – a atual Comissão Nacional de Proteção de Dados (CNPD).

Em 1998, foi aprovada a Lei de Proteção de Dados Pessoais – Lei nº 67/98, que transpôs a Diretiva 95/46/CE. No mesmo mês, foi aprovada a Lei nº 69/98, que veio regular a proteção de dados pessoais e a defesa da privacidade no setor das telecomunicações, transpondo a Diretiva de Telecomunicações (Diretiva 97/66/CE). As Lei nº 10/91 e 28/94 foram revogadas pela Lei nº 67/98.

Em 2004, a Lei nº 69/98 foi revogada com a publicação da Lei nº 41/2004, que regula a proteção de dados pessoais no setor das comunicações eletrônicas, transpondo a Diretiva 2002/58/CE (CNPD, 2019).

Em 2016, o Parlamento Europeu e o Conselho aprovaram a mais importante legislação sobre proteção de dados pessoais da atualidade, o Regulamento (UE) 2016/679, de 27 de

abril, Regulamento Geral de Proteção de Dados – RGPD (*General Data Protection Regulation* – GDPR), que será tema dos tópicos a seguir. O RGPD é a lei de privacidade e segurança mais rigorosa do mundo (Wolford, 2019).

Apesar de ter sido elaborada e aprovada pela União Europeia (UE), o RGPD impõe obrigações a empresas e organizações em qualquer lugar do mundo, desde que visem ou coletem dados relacionados a pessoas na EU (Wolford, 2019).

A partir de 25 de maio de 2018, o RGPD se tornou aplicável em todo o mundo, devido a sua característica extraterritorial. Em Portugal, o RGPD se aplica integralmente e automaticamente, pois é um país membros da UE, e por se tratar de um "Regulamento" – que vincula a sua aplicação integral a todos os Estados membros (Europa.eu, 2019).

Enfim, para se entender o panorama da privacidade e da proteção de dados atualmente é preciso entender o RGPD, pois ele tem efeitos globais na atual forma de fazer negócios e no tratamento de dados pessoais.

3.5.2. Breve histórico e comentários ao Regulamento Geral de Proteção de Dados

Como já foi abordado em tópicos anteriores, o direito à privacidade se consolidou no último século e está presente nos principais documentos internacionais, bem como na legislação interna da maioria dos países. Na Europa, o direito à privacidade faz parte da Convenção Europeia dos Direitos Humanos de 1950, que em seu art. 8º diz: "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". A partir dessa premissa, a União Europeia procura proteger esse direito através da sua legislação.

Com a evolução da tecnologia e o surgimento da internet, a UE percebeu a necessidade de uma legislação moderna para a proteção da privacidade. Assim, em 1995, a UE aprovou a Diretiva 95/46/CE (Diretiva Europeia de Proteção de Dados), que estabeleceu padrões mínimos de privacidade e segurança de dados. Com base nessa Diretiva, cada Estado membro criou sua própria lei de implementação.

Mas a evolução da internet foi rápida. Em 1994, o primeiro banner publicitário apareceu online. Em 2000, a maioria das instituições financeiras ofereciam serviços bancários on-line. Em 2006, o Facebook abriu ao público. Em 2011, um usuário do Google processou a empresa por verificar seus e-mails. Dois meses depois, começaram os trabalhos para atualizar a diretiva de 1995. Desse trabalho surgiu o RGPD, que entrou em vigor em 2016 e se tornou aplicável desde 25 de maio de 2018 (Wolford, 2019).

Por ser a legislação mais importante sobre a matéria, importa fazer uma breve análise do RGPD no que for pertinente ao tema deste trabalho. A seguinte análise é baseada nos comentários do livro de Nóbrega Maldonado e Opice Blum (2018).

No art. 1º já podemos identificar o objeto e principais objetivos da legislação, que busca proteger o direito das pessoas naturais, no que diz respeito ao tratamento de seus dados pessoais, bem como, a livre circulação desses dados.

Obviamente, o principal foco da RGPD é proteger os direitos e garantias fundamentais dos cidadãos, com objetivo de diminuir os riscos da coleta e uso, compartilhamento, armazenamento, entre outros, dos dados pessoais.

No entanto, tudo isso deve ser posto em prática sem que o regulamento impossibilite o desenvolvimento de novos modelos de negócios baseados na atual sociedade da informação tecnológica, onde os dados pessoais são substrato para gerar valor na maioria das empresas, desde as pequenas às grandes corporações.

Assim, o RGPD não pretende inviabilizar o progresso econômico e social, mas antes criar um ambiente de liberdade, segurança e justiça, como se pode observar no Considerando 2. Ou seja, a criação de uma Lei Geral de proteção de dados, em consonância com a RGPD, consolida uma nação como um "porto seguro" para investimento. Essa segurança jurídica, trazida por limites claros do que é permitido e proibido, quais as responsabilidades das empresas, os riscos e as sanções a que estão sujeitas, atrai investidores internos e externos que procuram regras claras e similares ao que está sendo adotado no mundo.

Dessa forma, o RGPD pretende proteger os dados pessoais em geral, dando aos titulares o controle e compreensão sobre tudo que acontece com seus dados pessoais durante todo ciclo de tratamento (coleta, uso, compartilhamento, armazenamento, até a exclusão), sem que isso gere impactos negativos nos novos modelos de negócios.

O art. 2º traz o âmbito de aplicação material do Regulamento. O RGPD se aplica ao tratamento de dados pessoais, quer seja por meios total ou parcialmente automatizados, quer seja por meios não automatizados em dados pessoais contidos em arquivos ou que visem a formação de arquivos.

No art. 2º (2), o RGPD assinala as situações em que o Regulamento não será aplicado. Aqui é importante ressaltar as situações elencadas nas alíneas "a" e "d", que se relacionam diretamente com o tema deste trabalho. Com isso, não se aplica o RGPD ao tratamento de dados pessoais:

1) "a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União" – aqui estão incluídas atividades relacionadas à segurança pública e à defesa nacional, conforme explica o Considerando 16[2] do RGPD;
2) "d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública" – conforme Considerando 19[3] da RGPD, essa matéria é regulamentada pela Diretiva 2016/680 – Diretiva Relativa à Proteção dos Dados Destinados às Autoridades Policiais e Judiciais (*Law Enforcement Data Protection Directive* – LED).

Apesar de não ser mais necessário discorrer tanto sobre o RGPD, uma vez que ele não se aplica aos casos descritos acima, é importante frisar uma das maiores mudanças que essa legislação trouxe em relação à Diretiva anterior de 1995: a aplicabilidade extraterritorial.

No art. 3º, o RGPD explica a aplicação territorial da lei. O primeiro critério é de que qualquer estabelecimento que esteja fisicamente situado no território da UE, independentemente de o tratamento ocorrer dentro ou fora da União, estará sujeito à aplicação do Regulamento.

Outro critério é a aplicação do Regulamento às empresas que não estejam situadas no espaço da UE, mas que ofereçam bens ou serviços aos titulares que se encontrem fisicamente no território do União, mesmo que não haja cobrança de valores. Ou seja, não importa a

[2] UE. RGPD, considerando 16: O presente regulamento não se aplica às questões de defesa dos direitos e das liberdades fundamentais ou da livre circulação de dados pessoais relacionados com atividades que se encontrem fora do âmbito de aplicação do direito da União, como as que se prendem com a segurança nacional. O presente regulamento não se aplica ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relacionadas com a política externa e de segurança comum da União.

[3] UE. RGPD, considerando 19: A proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos. Todavia, os dados pessoais tratados pelas autoridades competentes ao abrigo do presente regulamento deverão ser regulados, quando forem usados para os efeitos referidos, por um ato jurídico da União mais específico, a saber, a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho (1). Os Estados-Membros podem confiar às autoridades competentes na acepção da Diretiva (UE) 2016/680 funções não necessariamente a executar para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, de modo a que o tratamento dos dados pessoais para esses outros efeitos, na medida em que se insira na esfera do direito da União, seja abrangido pelo âmbito de aplicação do presente regulamento.

cidadania do titular nem de que lugar do planeta seja a empresa, basta que o bem ou serviço oferecido seja a alguém que esteja em território da UE para que haja a aplicação do RGPD.

Além disso, o Regulamento também é aplicado quando houver o monitoramento do "controle do comportamento"[4] de titulares que estejam na União, mesmo que o responsável por esse controle não esteja fisicamente na UE, sendo esse mais um exemplo de aplicação extraterritorial.

Por fim, também haverá aplicação do RGPD nos casos em que o responsável pelo tratamento esteja estabelecido em local em que se aplique a legislação da UE por força do direito internacional público, por exemplo em missões diplomáticas ou em postos consulares de um Estado-Membro. Assim, embaixadas dos países membros da União Europeia devem cumprir o que está previsto no RGPD (Nóbrega Maldonado e Opice Blum, 2018).

Como foi observado, o RGPD não se aplica às autoridades competentes para a prevenção de infrações criminais, conforme exceção disposta no artigo 2º do Regulamento. Dessa forma, importa realizar a análise da Diretiva especifica sobre esse assunto.

3.5.3. Atual conjuntura em Portugal

Para o caso de Portugal, país membro da UE, temos que entender a conjuntura atual para melhor realizar o estudo do tema. Primeiro, cabe explicar como funciona alguns atos legislativos da União Europeia. No momento em que foi aprovado e publicado o RGPD, também foram publicadas duas Diretivas relativas ao tema da proteção dos dados pessoais: a Diretiva 2016/680, relativa à proteção dos dados destinados às autoridades policiais e judiciais; e a Diretiva (UE) 2016/681, sobre dados de identificação de passageiros (PNR) para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave.

O RGPD, por ser um Regulamento, "é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da UE" (Europa.eu, 2019). Ou seja, no momento em que um Regulamento é aprovado e entra em vigor, todos os países membros são

[4] UE. RGPD, considerando 24: A fim de determinar se uma atividade de tratamento pode ser considerada «controle do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.

obrigados a adotar as suas regras. No caso da Diretiva, ela é um "ato legislativo que fixa um objetivo geral que todos os países da UE devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objetivo" (Europa.eu, 2019). Ou seja, para que uma Diretiva entre em vigor em um país membro da UE, esse país deve promulgar uma lei própria para transpor a Diretiva.

Foi o caso da Lei nº 21/19, que conforme descrição do seu sumário: "regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados, *transpondo a Diretiva (UE) 2016/681* do Parlamento Europeu e do Conselho, de 27 de abril de 2016". Dessa forma, os objetivos da Diretiva (UE) 2016/681 passam a ser cumpridos em Portugal através da referida lei.

Contudo, até a presente data (03/07/19), a Diretiva (UE) 2016/680 ainda não tinha sido transposta. Um comunicado foi publicado pela CNPD de Portugal em 25 de maio de 2018, dizendo que a partir dessa data "o RGPD tem plena aplicação em toda a União Europeia e, por isso, também em Portugal". E continua: "No que diz respeito aos tratamentos de dados pessoais relativos à prevenção, investigação e repressão criminal, a Lei n.º 67/98 tem integral aplicação, sem qualquer alteração, até à transposição da Diretiva 2016/680" (CNPD, 2018). Assim, para o tratamento de dados pessoais por parte das autoridades policiais, atualmente, se aplica a Lei 67/98 – Lei de Proteção de Dados Pessoais.

Existe a Proposta de Lei nº 125/XIII que pretende transpor a Diretiva (UE) 2016/680, mas ainda se encontra em tramitação na Assembleia da República (Assembleia da República, 2018).

Por fim, o relatório do Grupo sobre a regulação da Diretiva (UE) 2016/680, da Comissão Europeia, publicou, em 12/04/19, a atualização da situação de cada país membro da UE em relação à transposição dessa Diretiva (European Commission, 2019). Em relação à Portugal, relatou que o governo propôs uma lei especifica para transpor a Diretiva (UE) 2016/680, e que essa proposta legislativa foi aprovada pelo Conselho de Ministros em 12/04/18. O relatório aponta que essa proposta se encontra no parlamento para discussão e aprovação, sendo esperado a sua aplicação a partir de julho de 2019.

Descrito este panorama atual da legislação portuguesa, verifica-se que a Diretiva que trata especificamente do tratamento de dados pessoais por parte das autoridades policiais, ainda não foi transposta, mas existe a expectativa que ela seja transposta ainda em 2019. Ou seja, aplica-se a Lei nº 67/98, sobre a proteção de dados pessoais, até que a Diretiva seja transposta.

Diante dessa conjuntura de transição, e na expectativa da aprovação de uma lei que irá transpor a Diretiva (UE) 2016/680, ainda no ano de 2019, este trabalho irá analisar a regras estabelecidas pela Diretiva, pois o objetivo é confrontar o direito à privacidade e à segurança de acordo com as regras mais atualizadas.

3.5.4. Análise da Diretiva (UE) 2016/680 (LED)

Neste tópico, serão analisados os artigos mais relevantes da Diretiva (UE) 2016/680 para o tema proposto nesse trabalho, separados por capítulos.

3.5.4.1. Capítulo I – Disposições Gerais

A Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que foi publicada juntamente com o RGPD, trata da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, conforme estabelecido em seu artigo 1º.

Também conhecida como LED (*Law Enforcement Directive*), se refere ao tratamento de dados por parte das autoridades policiais. No que se refere à tecnologia de reconhecimento facial em câmeras CFTV, ela corresponde a praticamente todos os termos do conceito, pois auxilia as autoridades competentes na prevenção, na investigação e na detecção de infrações penais.

Quanto à prevenção, o sistema de reconhecimento facial pode evitar o acontecimento de um crime, através do monitoramento e da ação rápida dos agentes em campo, bem como, através do simples conhecimento da existência de câmeras, que pode inibir a ação de criminosos. Na investigação, o sistema pode procurar a face de um indivíduo suspeito de cometer um crime na base de dados, podendo chegar à gravação do próprio cometimento do crime. Referente à detecção, o sistema é capaz de ler automaticamente os rostos dos transeuntes, pesquisando criminosos procurados pela justiça, e alertando automaticamente quando o indivíduo é localizado.

O art. 1º ainda prevê que os Estados-Membros devem assegurar a proteção dos direitos e das liberdades fundamentais das pessoas, especialmente o direito à proteção de dados pessoais, não impedindo que o Estado-Membro preveja garantias mais elevadas do que as previstas na Diretiva.

O art. 2º delimita o âmbito de aplicação da Diretiva, sendo relativa apenas ao tratamento de dados pessoais realizados pelas autoridades competentes para os efeitos descritos no artigo 1º, ou seja, que visem a prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, que são os casos das autoridades policiais.

O art. 3º traz o rol de definições que são utilizadas pela Diretiva. Essas definições são as mesmas utilizadas pelo RGPD, sendo suprimidas algumas definições e acrescentado o termo "Autoridade competente". Aqui serão expostas as principais definições:

- Dados pessoais: "informações relativas a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular";
- Tratamento: "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição";
- Definição de perfis: "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações";
- Autoridade competente:

  a) "uma autoridade pública competente para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública"; ou

  b) "qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer a autoridade pública e os poderes públicos para efeitos de

prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública";

- Responsável pelo tratamento: "a autoridade competente que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais; caso as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou pelo direito de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro";
- Dados biométricos: "dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos".

3.5.4.2. Capítulo II – Princípios

No art. 4º são elencados os princípios relativos ao tratamento de dados pessoais que devem ser perseguidos pelos Estados-Membros. Os dados pessoais devem ser:

a) "Objeto de um tratamento lícito e leal;
b) Recolhidos para finalidades determinadas, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades;
c) Adequados, pertinentes e limitados ao mínimo necessário relativamente às finalidades para as quais são tratados;
d) Exatos e atualizados sempre que necessário; devem ser tomadas todas as medidas razoáveis para que os dados inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora;
e) Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados;
f) Tratados de uma forma que garanta a sua segurança adequada, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas";

Esse artigo norteia todo o processo de tratamento de dados pessoais por parte das autoridades policiais. Conforme art. 8º, um tratamento só é lícito se e na medida em que for

necessário para o exercício de uma autoridade competente para os efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais. Assim, quando do tratamento dos dados pessoais, a autoridade competente deve sempre estar focada no objetivo de sua missão e no efeito desejado, para não se desviar da licitude do procedimento.

Importante ressaltar o item que cita a finalidade. Os dados devem ser recolhidos de acordo com uma finalidade previamente determinada, explícita e legítima, devendo todo o ciclo do tratamento dos dados pessoais ter foco nessa finalidade, pois quando um dado não for mais necessário para se alcançá-la, ele deve ser excluído.

O art. 5º cita que os Estados-Membros devem prever prazos adequados para os dados pessoais serem apagados ou para a avaliação periódica da necessidade de os conservar. O artigo não estipula um prazo fixo, tão somente cita que eles devem ser "adequados". Assim, cada país deve estipular suas regras de conservação dos dados e prever regras para que eles sejam cumpridos.

O art. 6º traz algo bem específico aos responsáveis pelo tratamento de dados pessoais a que se destina a Diretiva, que é a categorização dos titulares dos dados. Se aplicável, e na medida do possível, os Estados-Membros devem prever uma clara distinção entre os dados pessoais de diferentes categorias de titulares de dados (suspeitos, condenados, vítimas, testemunhas):

a) "Pessoas relativamente às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal;
b) Pessoas condenadas por uma infração penal;
c) Vítimas de uma infração penal ou pessoas relativamente às quais certos fatos levam a crer que possam vir a ser vítimas de uma infração penal; e
d) Terceiros envolvidos numa infração penal, tais como pessoas que possam ser chamadas a testemunhar em investigações penais relacionadas com infrações penais ou em processos penais subsequentes, pessoas que possam fornecer informações sobre infrações penais, ou contatos ou associados de uma das pessoas a que se referem as alíneas a) e b)".

O art. 10º aborda o tratamento de categorias especiais de dados pessoais, que é o caso dos dados biométricos como a face, objeto desse estudo. O tratamento desse tipo de dado pessoal somente é autorizado se for estritamente necessário, se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados, e se: "a) for autorizado pelo direito da União ou de um Estado-Membro; b) se destinar a proteger os interesses vitais do titular

dos dados ou de outra pessoa singular; ou c) estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados".

No caso do reconhecimento facial por câmeras utilizadas por autoridades policiais, o órgão competente deverá se enquadrar a esse artigo, quando for estipular a finalidade do tratamento, devendo ser estritamente necessário e garantir a proteção dos direitos do titular por todos os meios. Além disso, deve cumprir uma das três alíneas que constam no artigo. Para além da autorização que o próprio Estado-Membro conceder, a utilização de câmeras de reconhecimento facial em locais públicos pode encontrar abrigo na alínea "c", pois os dados são manifestamente tornados públicos pelo titular dos dados.

O art. 11º prevê a proibição de decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos adversos ao titular dos dados, a menos que seja autorizado pelo direito da União ou do Estado-Membro, devendo prever garantias adequadas dos direitos e liberdades do titular, com pelo menos o direito de obter a intervenção humana do responsável pelo tratamento. E ainda, proíbe a definição de perfis que conduza à discriminação de pessoas com base nos dados especiais referidos no artigo 10º, como o dado biométrico.

Assim, para o reconhecimento facial, as decisões devem ser tomadas em conjunto com o responsável pelo tratamento, e, caso seja autorizado pelo país a decisão com base no tratamento automatizado, o titular deve ter o direito à intervenção humana do responsável pelo tratamento. Para além disso, é proibido a definição de perfis, com base na tecnologia de reconhecimento facial, que conduzam à discriminação de pessoas.

3.5.4.3. Capítulo III – Direito do Titular dos Dados

Neste capítulo são apresentados os direitos do titular dos dados. Apesar dessa Diretiva ser uma exceção ao RGPD, as autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, também, devem garantir uma série de direitos aos titulares dos dados.

O art. 12º trata da comunicação e regras de exercício dos direitos dos titulares dos dados. Os Estados-Membros devem tomar todas as medidas razoáveis para fornecer ao titular dos dados informações constantes no art. 13º (explicado no parágrafo a seguir), bem como efetue todas as comunicações previstas da Diretiva, utilizando uma linguagem clara e simples, inclusive por meios eletrônicos.

O art. 13º traz as informações que devem ser facultadas ou fornecidas ao titular dos dados, sendo pelo menos: "a) A identidade e os contatos do responsável pelo tratamento; b) Os contatos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam; d) O direito de apresentar reclamação à autoridade de controle e de obter os contatos dessa autoridade; e) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que dizem respeito ao titular, bem como a sua retificação ou o seu apagamento e a limitação do tratamento".

Além dessas informações, em determinados casos, os Estados-Membros devem prever em lei o fornecimento de informações adicionais, a fim de permitir o exercício dos direitos do titular, tais como: "a) O fundamento jurídico do tratamento; b) O prazo de conservação dos dados pessoais ou, se tal não for possível, os critérios usados para definir esse período; c) Se aplicável, as categorias de destinatários dos dados pessoais, inclusive nos países terceiros ou nas organizações internacionais; d) Se for caso disso, informações adicionais, especialmente se os dados pessoais forem recolhidos sem conhecimento do seu titular".

Percebe-se que o titular dos dados tem o direito de ter conhecimento de todo o ciclo de tratamento de seus dados pessoais, tendo um papel protagonista no processo, sendo-lhe garantido informações como a finalidade do tratamento, seu fundamento jurídico, prazo de conservação, contatos do responsável e etc.

Além do direito à informação, o titular dos dados tem o direito ao acesso a seus dados, conforme dispõe o art. 14º. O titular tem direito, ainda, de confirmar se seus dados estão a ser tratados ou não, e, caso afirmativo, acessá-los, bem como, obter informações como a finalidade e o fundamento jurídico do tratamento, para quem foram divulgados os dados, o prazo previsto para conservação, o direito de reclamação à autoridade de controle, entre outros.

O art. 15º explica em que situações os Estados-Membros podem limitar, total ou parcialmente, o direito do titular de acessar seus dados pessoais, desde que constitua uma medida necessária e pautada em uma sociedade democrática, tendo em conta os direitos fundamentais e os interesses legítimos das pessoas em causa, com a finalidade de:

a) "Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;
b) Evitar prejudicar a prevenção, detecção, investigação ou repressão de infrações penais ou a execução de sanções penais;
c) Proteger a segurança pública;
d) Proteger a segurança nacional;

e) Proteger os direitos e as liberdades de terceiros".

Essas são as mesmas justificativas que fundamentam a limitação do fornecimento de informações ao titular, previstos no art. 13º. Para o reconhecimento facial, as imagens armazenadas não estão identificadas como sendo de um determinado titular, apesar de serem identificáveis. Assim, para fornecer ao titular a informação de que seu dado está sendo tratado, deve se fazer uma varredura no sistema a procura do rosto do titular que deseja a informação ou o dado. Devido à dificuldade de fornecer esses dados, ainda mais que as imagens gravadas, normalmente, constam dados de outros titulares, o Estado-Membro pode se valer dessa limitação de fornecimento de informações e dados.

O art. 16º traz o direito do titular ao apagamento de seus dados pessoais, caso responsável pelo tratamento infrinja as disposições dos artigos 4º (princípios relativos ao tratamento de dados pessoais), 8º (licitude do tratamento) ou 10º (categorias especiais de dados pessoais). O responsável pelo tratamento pode se recusar a apagar os dados com base nos mesmos argumentos do art. 15º, citados acima.

3.5.4.4. Capítulo IV – Responsável pelo tratamento e subcontratante

Neste capítulo são abordadas obrigações gerais do responsável pelo tratamento de dados pessoais.

No artigo 19º expõe que os responsáveis pelo tratamento de dados pessoais devem aplicar medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento é realizado de acordo com a Diretiva. Esse artigo reforça a responsabilidade para com os dados pessoais, tendo que se aplicar todas as medidas de segurança possíveis para garantir a proteção desses dados.

O art. 20º traz o conceito de proteção de dados "*by design and by default*", trazido também pelo RGPD. O responsável pelo tratamento deve aplicar, tanto no momento da definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas concebidas para aplicar de forma eficaz os princípios da proteção de dados, a fim de satisfazer os requisitos da Diretiva e de proteger os direitos dos titulares dos dados.

Além disso, ainda conforme o artigo, o responsável pelo tratamento deve aplicar as medidas técnicas e organizativas adequadas para assegurar que apenas são tratados os dados pessoais necessários para cada finalidade específica do tratamento. Isso se aplica ao volume

de dados pessoais recolhidos, à extensão do seu tratamento, ao prazo de conservação e à sua acessibilidade.

Assim, para uma possível implementação de tecnologia de reconhecimento facial, deve se levar em conta, desde o momento em que se define os meios de tratamento, as medidas que devem ser adotadas para garantir a aplicação total da Diretiva 2016/680, bem como, restringir o tratamento das imagens ao estritamente necessário para o cumprimento de sua finalidade. Isso deve ser levando em conta também para se definir o prazo de conservação dos dados e para não disponibilizar acesso aos dados à um número indeterminado de pessoas.

O art. 24º explica que os responsáveis pelo tratamento devem manter um registro de todas as categorias de atividades de tratamento sob sua responsabilidade, trazendo um rol de dados que devem constar nesse registro.

O art. 25º cita que os sistemas de tratamento automatizados, como o do reconhecimento facial, devem manter registros cronológicos de operações de recolha, alteração, consulta, divulgação, interconexão e apagamento de dados. Esses registros são utilizados exclusivamente para efeitos de verificação da licitude do tratamento, autocontrole e garantia da integridade e segurança dos dados pessoais, bem como para ações penais.

O art. 27º traz a previsão da avaliação de impacto sobre a proteção de dados. Ele diz que, caso um tipo de tratamento, em particular que utiliza novas tecnologias, seja suscetível de resultar em um elevado risco para os direitos e liberdades individuais, o responsável deve efetuar, antes do início do tratamento, uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais.

Essa avaliação, segundo o artigo, deve conter uma descrição geral das operações de tratamento de dados previstas; uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados; as medidas previstas para fazer face a esses riscos; as garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais; e demonstrar a conformidade com a diretiva, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

No tocante à implementação da tecnologia de reconhecimento facial, essa avaliação é de suma importância. Por ser uma solução tecnológica com implementação ainda restrita no Ocidente, e diante da inovação legislativa dessa Diretiva, a avaliação de impacto traz segurança para o responsável pelo tratamento, para o titular dos dados e para os órgãos de controle, sendo essencial para o sucesso do projeto.

O art. 30º traz a obrigação do responsável pelo tratamento de notificar, em até 72 horas após o conhecimento, os casos de violação de dados pessoais à autoridade de controle.

3.5.4.5. Capítulo VI – Autoridades de controle independentes

Por fim, o capítulo VI traz uma série de artigos relacionados à autoridade de controle, cabendo ressaltar dois deles.

O art. 41º relata que cabe a uma ou mais autoridades públicas independentes (autoridade de controle) a responsabilidade de fiscalizar a aplicação da Diretiva, a fim de proteger os direitos e liberdades fundamentais das pessoas relativamente ao tratamento de dados pessoais e de facilitar a livre circulação desses dados na União. Essa autoridade deve ser a mesma autoridade de controle prevista no RGPD. O art. 42º, por sua vez, reforça que essa autoridade de controle deve agir com total independência no exercício das usa atribuições.

Em Portugal essa autoridade existe desde 1994, se trata da Comissão Nacional de Proteção de Dados – CNPD. Antes com o nome de CNPDPI, mas com a atual designação desde a aprovação da Lei nº 67/98, a CNPD é a Autoridade Nacional de Controle de Dados Pessoais.

Uma entidade administrativa independente, ela é responsável por controlar e fiscalizar o processamento de dados pessoais, de acordo com os preceitos da Constituição e das leis, bem como, em respeito aos direitos do homem, suas liberdades e garantias (Comissão Nacional de Proteção de Dados, 2019).

3.5.5. Lei sobre câmeras de videovigilância

Além do RGPD e da Diretiva (UE) 2016/680, Portugal possui uma lei infraconstitucional pertinente ao tema desse trabalho, a Lei nº 1/2005, de 10 de janeiro, que regula a utilização de câmeras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum.

Para que sistemas de câmeras de reconhecimento facial sejam utilizados em Portugal pelas forças de segurança, é necessário se adequar tanto à Diretiva (UE) 2016/680 quanto à Lei nº 1/2005.

Será feita uma breve análise dos principais artigos da referida lei, a fim de se entender as exigências legais para instalação de câmeras em locais públicos pelas forças de segurança.

O art. 1º traz o objetivo da lei, que é regular a "utilização de sistemas de vigilância por câmeras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, para captação e gravação de imagem e som e seu posterior tratamento". Essa regulação engloba câmeras utilizadas para o reconhecimento facial, pois seriam câmeras instaladas em locais públicos e utilizadas pelas forças de segurança.

O art. 2º explica para quais finalidades são autorizadas a utilização de videovigilância, sendo elas: "a) Proteção de edifícios e instalações públicos e respectivos acessos; b) Proteção de instalações com interesse para a defesa nacional; c) Proteção da segurança das pessoas e bens, públicos ou privados, e prevenção da prática de crimes em locais em que exista razoável risco da sua ocorrência".

Para o caso dos sistemas de reconhecimento facial no contexto deste trabalho, fica clara a opção a ser utilizada pelas forças de segurança, a alínea "c". Mas importa ressaltar que, nos casos em que a finalidade é a prevenção criminal, é necessário que exista razoável risco de ocorrência da prática de crimes no local em que se pretende instalar as câmeras.

O art. 3º exige, para instalação de câmeras fixas, a autorização do membro do Governo que tutela a força de segurança, precedido de parecer da Comissão Nacional de Proteção de Dados (CNPD).

O art. 4º explica em que condições estas câmeras fixas devem ser instaladas, exigindo que seja afixado, em local bem visível, informações sobre: "a) A existência e a localização das câmaras de vídeo; b) A finalidade da captação de imagens e sons; c) O responsável pelo tratamento dos dados recolhidos, perante quem os direitos de acesso e retificação podem ser exercidos".

Verifica-se que, apesar da lei ser anterior ao RGPD, Portugal já se preocupava a muito tempo com a proteção de dados, pois esse artigo vai ao encontro dos ideais do Regulamento e da Diretiva (UE) 2016/680, no que se refere a transparência e informação ao titular sobre o tratamento de seus dados.

O art. 7º traz uma série de princípios a ser seguidos quando da utilização de câmeras de videovigilância, onde cabe ressaltar dois deles: princípios da proporcionalidade e da adequabilidade. A utilização de câmeras de vídeo é autorizada somente quando se mostrar um meio proporcional e mais adequado para se manter a segurança e a ordem públicas e para prevenir a prática de crimes, de acordo com as circunstâncias concretas do local a ser vigiado.

Denota-se a preocupação do legislador no que se tange a instalação desenfreada de câmeras de videovigilância em locais públicos. A ideia não é uma sociedade completamente

vigiada pelas forças de segurança, e sim, que as câmeras sejam ferramentas para alcançar a finalidade da paz social.

Por fim, importante destacar o art. 9º, que estipula o prazo máximo de um mês para conservação das imagens de câmeras instaladas de acordo com essa lei. Essa lei, caso não seja revogada pela lei que irá transpor a Diretiva (UE) 2016/680, limita o tempo de conservação de imagens de sistemas de videovigilância com a tecnologia de reconhecimento facial. Essa limitação vai ao encontro da própria Diretiva (UE) 2016/680, que diz que cada país deve prever prazos adequados para conservação dos dados pessoais, não estipulando um prazo fixo.

3.6. Proteção de dados no Brasil

O Brasil não tem tanta história legislativa sobre proteção de dados como Portugal. De forma ainda muito superficial, o assunto foi tratado somente em 2014 com a aprovação da Lei nº 12.965/14, conhecida como o Marco Civil da Internet.

Mas essa lei não era suficiente para assegurar a proteção dos dados pessoais, ainda mais com a evolução da sociedade tecnológica em que se vive. Foi então que, em 14 de agosto de 2018, e com base na regulamentação europeia sobre proteção de dados – RGPD, o Brasil criou a Lei Geral de Proteção de Dados (LGPD), através da Lei nº 13.709/18, alterada pela Lei nº 13.853, de 8 de julho de 2019.

3.6.1. Conceitos iniciais da LGPD

Neste tópico serão abordados os conceitos fundamentais da LGPD. Este tópico é baseado no livro escrito por Patrícia Pinheiro (2018).

O objetivo principal da LGPD é resguardar os direitos fundamentais da liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, no que se refere ao tratamento de dados pessoais. Ela traz vários princípios que devem ser seguidos por aqueles que pretendem tratar dados pessoais, bem como, diversos itens de controle técnico para segurança da informação.

A inspiração para o aparecimento de regulamentações sobre proteção de dados pessoais está diretamente ligada ao desenvolvimento da forma de negócios da economia digital atual, que de forma mais sólida, a partir da década de 1990, passou a depender cada vez mais dos fluxos internacionais de bases de dados, impulsionado pela globalização e pelos avanços tecnológicos.

A principal iniciativa para o desenvolvimento do tema "proteção de dados" partiu da União Europeia (UE), que aprovou o Regulamento Geral de Proteção de Dados Pessoais Europeu (RGPD), em 27 de abril de 2016, com o intuito de proteger o direito das pessoas no que se refere ao tratamento de dados pessoais e a sua livre circulação (*free data flow*). O RGPD entrou em vigor no dia 25 de maio de 2018 e causou uma espécie de "efeito cascata", uma vez que o regulamento exige que outros países e empresas que pretendem manter relações comerciais com a UE também devem ter uma legislação do mesmo nível do RGPD, sob pena do Estado que não cumprir esse requisito sofrer algum tipo de barreira econômica ou dificuldade de negociar com países da UE.

A proteção dos dados pessoais é considerada um direito fundamental em muitos países. Na Europa, já estava definida na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia. No Brasil, essa proteção estava prevista nas leis do Marco Civil da Internet e do Cadastro Positivo, contudo, ainda era apreciada de forma difusa e sem objetividade, quanto ao tratamento dos dados, não sendo possível aferir um mínimo de segurança das informações. A LGPD veio para inovar nesse sentido, pois normalizou padrões de qualidade objetivos que devem ser seguidos por todos que pretendem tratar dados pessoais no Brasil.

Alguns conceitos adotados pela LGPD são importantes para a discussão do tema. Segundo o art. 5º da lei nº 13.709/18 (LGPD), são alguns desses conceitos:

- Titular: "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento";
- Tratamento: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração";
- Dado pessoal: "informação relacionada a pessoa natural identificada ou identificável";
- Dado pessoal sensível: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural";

- Consentimento: “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”;
- Controlador: “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”;
- Operador: “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”;
- Agentes de tratamento: “o controlador e o operador”;
- Encarregado: “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)”.

A LGPD, conforme art. 3º, é aplicada a todos que realizem tratamentos de dados pessoais, sejam pessoas físicas ou jurídicas, organizações públicas ou privadas, independentemente do meio, do país da sua sede ou do país onde esteja localizado os dados, desde que cumpra qualquer um dos seguintes requisitos:

1) “a operação de tratamento seja realizada no território nacional;
2) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
3) os dados pessoais objeto do tratamento tenham sido coletados no território nacional”.

Dessa forma, a aplicação da LGPD não está relacionada à cidadania ou à nacionalidade dos dados pessoais, nem à residência do titular. Assim como a RGPD, ela tem alcance extraterritorial, isto é, efeitos internacionais, pois se aplica a todos que realizem tratamento de dados pessoais e que cumpram os requisitos supramencionados, mesmo que sediados em outros países (Pinheiro, 2018).

3.6.2. Análise da LGPD

Este tópico tem o objetivo de comentar os principais artigos da LGPD referentes ao tema desse trabalho. Este tópico é baseado no livro escrito por Patrícia Pinheiro (2018).

Os artigos 1º, 2º e 3º tratam principalmente do objetivo, dos fundamentos e das regras de aplicação da LGPD, os quais já foram, de alguma maneira, comentados no tópico anterior.

O art. 4º traz uma importante redação, a qual se deve estar atento: as hipóteses de exceção à aplicação da lei. A LGPD não se aplica ao tratamento de dados pessoais: "(i) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; (ii) para fins exclusivamente: a) jornalísticos e artísticos, ou b) acadêmicos […]; (iii) realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais; […]".

Para os casos pontuados no item (iii), de acordo com o §1° do art. 4º, estes serão redigidos por lei específica, atendendo o interesse público, o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD. Além disso, a Autoridade Nacional de Proteção de Dados (ANPD), irá emitir recomendações e opiniões técnicas e solicitar relatórios de impacto à proteção de dados.

E ainda, o §4° proíbe o tratamento dos dados pontuados no item (iii) por pessoa de direito privado, salvo as que possuem capital integralmente constituído pelo poder público.

Através dessas restrições impostas aos tipos de tratamento de dados que são regulados pela LGPD, a lei visa limitar o seu próprio alcance. Dessa forma, a lei expressa que, apesar do tratamento de dados pessoais ter seu lugar de direito a ser respeitado e protegido, este não deve superar a liberdade de informação e expressão, a soberania, a segurança e a defesa do Estado.

Além de contribuir para a redução de impactos econômicos e sociais, inerentes a implementação das exigências da LGPD, o artigo 4º equilibra a proteção da privacidade (direito individual) e a proteção da segurança pública (direito coletivo), principalmente ante os deveres atuais de se combater o crime organizado, a fraude digital e o terrorismo.

O artigo 6º cita que as atividades de tratamento de dados pessoais devem observar a boa-fé e seguir os princípios: da finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas. São princípios norteadores de todas as ações dos responsáveis por tratamento de dados pessoais.

O artigo 7º trata das hipóteses em que poderá ser realizado o tratamento de dados pessoais, sendo a principal o consentimento do titular. Cabe ressaltar o §4° desse artigo que dispensa a exigência do consentimento para os dados tornados manifestamente públicos pelo titular, resguardados seus direitos e os princípios previstos na LGPD.

O art. 11º cita as hipóteses de tratamento de dados pessoais sensíveis, dentre eles os dados biométricos, como a face detectada por câmeras de reconhecimento facial. Mais uma vez a regra é o consentimento do titular ou responsável legal, de forma específica e destacada, para finalidades específicas.

Contudo, o inciso II do artigo 11º traz exceções à regra. Nas situações em que for indispensável ao cumprimento de obrigações legais por parte do controlador, à garantia da segurança do titular, à prevenção à fraude, à execução de políticas públicas, à proteção da vida/incolumidade física, bem como à tutela da saúde, não é necessário o consentimento. Mesmo que seja dispensado o consentimento para o tratamento de dados sensíveis, é obrigatório ao controlador dar publicidade a essa situação.

O art. 15º demonstra os casos em que ocorre o término do tratamento dos dados. Para a LGPD, o limite para o tratamento de dados pessoais é um requisito de validade do procedimento. Esse limite é tanto para as informações a serem coletadas quanto à finitude do processo no tempo.

Ou seja, o tratamento de dados pessoais não deve ser feito por tempo indeterminado. O art. 15º pontua as hipóteses de término do tratamento de dados pessoais, onde se destaca a verificação do alcance da finalidade do processo, o fim do período estimulado ao tratamento, a revogação do consentimento do titular e a determinação da ANPD.

O art. 17º vem para assegurar que a pessoa natural é titular de seus dados pessoais e tem garantidos seus direitos fundamentais de liberdade, de intimidade e de privacidade. Esse é um objetivo da LGPD, proteger o livre desenvolvimento da personalidade através da garantia desses direitos. Esse artigo é diretamente relacionado aos artigos 5º, X[5], da Constituição Federal e 21 do Código Civil[6].

O art. 23º inicia o Capítulo IV do dispositivo legal, que aborda o tratamento de dados pessoais pelo Poder Público. Assim como as empresas privadas precisam apresentar uma finalidade clara e transparente para o tratamento de dados pessoais, a pessoa jurídica de direito público deve perseguir o interesse público enquanto atende a sua finalidade pública.

O art. 32º, também do capítulo IV, aborda a necessidade das instituições públicas realizarem o relatório de impacto à proteção de dados pessoais no âmbito da administração pública, uma vez que pode ser alvo de solicitação da ANPD, além dessa poder sugerir adoção

[5] BRASIL. Constituição da República Federativa do Brasil de 1988, Art. 5º: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: […] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[6] BRASIL. Código Civil, Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

de padrões e boas práticas nos tratamento de dados pessoais pelo Poder Público. A LGPD busca ser eficaz tanto para setor privado quanto para o setor público.

O art. 38º da LGPD cita que a ANPD pode determinar ao controlador a elaboração do relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis. No parágrafo único, explica que o relatório de impacto deve conter, no mínimo, "a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados".

O art. 46º reforça a necessidade dos agentes de tratamento adotarem medidas de segurança, técnicas e administrativas capazes de garantir a segurança e o sigilo dos dados pessoais, assegurando a integridade, a disponibilidade e a confidencialidade da informação ao longo de todo o ciclo de vida do dado.

O art. 48º relata o dever do controlador de comunicar à ANPD e ao titular, dentro de um prazo razoável, a ocorrência de incidentes de segurança referente aos dados pessoais. Esse dever de comunicação é um reflexo da boa-fé, transparência e responsabilização dos atos dos agentes de tratamento, sendo essencial para relação de confiança entre agentes de tratamento, titulares, ANPD e sociedade.

O art. 52º prevê a aplicação de sanções administrativas pela ANPD aos agentes de tratamento de dados que cometerem infrações previstas na LGPD. A previsão de sanções administrativas é fundamental para que todos os responsáveis pelo tratamento de dados pessoais fiquem atentos à importância de garantir a segurança das informações.

Assim a LGPD busca estimular a aplicação da lei de forma preventiva. As sanções vão desde advertências até a imputação de multa simples – que pode chegar a 2% do faturamento, com limite total de R$ 50 milhões de reais – e diária, além da suspensão das atividades relativas ao banco de dados, dentre outras (Pinheiro, 2018).

O Capítulo IX da LGPD (art. 55-A ao 58-B) aborda a criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, bem como as suas competências.

Dentre as competências da ANPD estão a de zelar pela proteção dos dados pessoais; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação; editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade; realizar auditorias, ou determinar sua realização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; entre outras.

A Autoridade Nacional de Proteção de Dados será um órgão essencial no processo de implementação das regras de proteção de dados no Brasil, pois se trata de uma legislação com um tema inovador para o país, com a qual as empresas e órgãos públicos ainda não estão acostumados a lidar. Diferente de Portugal, que possui esse órgão desde 1994, o qual já implementava regras de proteção de dados e que somente teve que se adequar às novas regras impostas pelo RGPD, o Brasil está começando à implementar regras sobre esse tema, e terá um longo caminho pela frente para adequação total da legislação.

A ANPD deverá ensinar como se deve cumprir a lei, através de diretrizes, regulamentos e procedimentos, bem como, fiscalizar o fiel cumprimento da lei. Por isso a importância do art. 55-B, que assegura a autonomia técnica e decisória à ANPD.

Quanto ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, a este compete propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, e para a atuação da ANPD; elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; entre outras.

Por fim, o art. 65º, e último, define a data em que a lei entra em vigor, sendo a partir de 28/12/2018 para os artigos que se referem à ANPD e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, e ainda, 24 meses após a data da sua publicação para os demais artigos. Ou seja, o início da vigência da LGPD será em agosto de 2020. Até lá, todos aqueles que realizam o tratamento de dados pessoais, quer seja por pessoa natural ou por pessoa jurídica de direito público ou privado, deverão se adequar às novas exigências da LGPD, no que couber.

3.6.3. Proteção de dados e o reconhecimento facial no Brasil

Percebe-se a grande diferença legislativa entre Brasil e Portugal no que se refere à proteção de dados pessoais. Enquanto Portugal tem uma legislação consolidada e atual, bem como, uma Autoridade Nacional de Proteção de Dados que existe há 25 anos, o Brasil somente verá a sua Lei Geral de Proteção de Dados em vigor em 2020, e sua Autoridade Nacional de Proteção de Dados acaba de ser criada por lei, mas ainda não foi implementada e nem existe de fato.

Portanto, existe uma diferença enorme na discussão sobre esse tema entre os dois países. Em Portugal, apesar de estar em um período de transição para aprovação da Diretiva (UE) 2016/680, é possível ter uma projeção do quadro legislativo para se discutir a

implementação de sistemas de reconhecimento facial em câmeras públicas pelas forças de segurança. Além disso, Portugal tem uma legislação especifica sobre instalação de câmeras de videovigilância, conforme foi abordado no tópico 3.5.5.

No Brasil, a legislação geral sobre proteção de dados é muito recente, e não está em vigor. E ainda, não existe qualquer lei específica sobre essa matéria para a segurança pública, como a Diretiva (UE) 2016/680. É por isso que o tema é pauta de discussões em audiências públicas e debates online, como no caso do Ministério Público do Distrito Federal e Territórios (MPDFT), que no dia 16 de abril deste ano promoveu Audiência Pública para debater o uso de ferramentas de reconhecimento facial (MPDFT, 2019); e no caso do debate online "Perspectivas regulatórias para o reconhecimento facial" (ConJur, 2019), promovido pelo Instituto Brasiliense de Direito Público (IDP), através do projeto Governance 4.0, no dia 06/05/19.

Este autor participou dessa audiência pública promovida pelo MPDFT, que também está disponível no Youtube (2019). Dessa audiência, cabe destacar a fala do Procurador Leonardo Roscoe Bessa, que expôs que o direito à proteção de dados pessoais, inclusive os dados sensíveis, apesar de ser um direito fundamental, não é um direito absoluto, ele pode ser conformado. Na realidade, segundo ele, não há direitos absolutos, sendo que os direitos se contrapõem de acordo com seus valores constitucionais.

O procurador segue explicando que a utilização do reconhecimento facial não ofende os direitos à privacidade e à imagem, desde que esteja de acordo com a LGPD. Nesse sentido, manifesta que não seria necessária uma legislação especifica para o reconhecimento facial, pois a LGPD e a ANPD, por enquanto, seriam suficientes para uma implementação inicial. Contudo, Bessa demonstra uma preocupação com uma vigilância absoluta por parte do Estado, ressaltando ser importante uma legislação especifica para a utilização por parte do poder público.

Para se implementar, no Brasil, a tecnologia de reconhecimento facial em câmeras instaladas em locais públicos e controladas pelas forças de segurança pública, esses órgãos devem se adequar com a legislação atual sobre proteção de dados, ou seja, a Lei Geral de Proteção de Dados Pessoais.

A LGPD somente entrará em vigor em agosto de 2020, mas enquanto isso, os órgãos públicos devem ir se adequando à legislação, para estar de acordo com a lei no momento em que passar a vigorar, e não ter que parar a prestação de alguns serviços por falta de adaptação à lei.

Alguns estados do Brasil já utilizam a tecnologia de reconhecimento facial, como a Bahia, que registrou uma prisão no carnaval de 2019 através do uso da tecnologia de reconhecimento facial, conforme exposto no tópico 2.4.4. Bem como o Rio de Janeiro, que também utilizou durante o carnaval, e mais recentemente, utilizou a tecnologia no esquema de segurança para os torcedores da final da Copa América (G1 Rio, 2019), no dia 07/07/19.

O estado de São Paulo também está experimentando a tecnologia na cidade de Campinas, com a expectativa que o sistema funcione associado à um aplicativo de celular, que irá informar o policial mais próximo sobre a detecção de algum suspeito realizado pelo reconhecimento de facial (Globoplay, 2019).

Esses estados, e aqueles que pretendem implementar a tecnologia de reconhecimento facial no Brasil, devem trabalhar para se conformar com a LGPD. Mas aqui cabe a seguinte pergunta: a LGPD impede a implantação da tecnologia de reconhecimento facial pelos órgãos de segurança pública? A partir da análise da LGPD, é possível se chegar a algumas conclusões.

O art. 4º da LGPD traz as hipóteses em que a lei não será aplicada para o tratamento de dados pessoais, dentre elas, quando "realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais".

No mesmo artigo, no §1°, cita que esses casos serão redigidos por lei específica, isto é, por uma lei similar à Diretiva (UE) 2016/680, voltada para os agentes de segurança pública e defesa nacional.

Assim, a LGPD não impede que os órgãos de segurança pública implantem a tecnologia de reconhecimento facial, pois a lei sequer se aplica para atividades com fins exclusivos de segurança pública e de repressão de infrações penais. Mas isso não significa que esses órgãos podem implementar o sistema como bem entenderem, pois o §3º do art. 4º esclarece que a ANPD irá emitir opiniões técnicas ou recomendações para esses casos, além de solicitar o relatório de impacto à proteção de dados.

Não é porque uma atividade tem uma finalidade exclusiva de segurança pública que o tratamento de dados será feito de qualquer forma, ainda que dentro da hipótese de exceção, o tratamento de dados deve seguir os princípios da LGPD.

Isso porque quando se exige o relatório de impacto à proteção de dados, o órgão está vinculado a uma série de exigências, como informar a metodologia utilizada para a coleta e para a garantia da segurança das informações, bem como, a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Portanto, os órgãos de segurança pública podem fazer uso das tecnologias de reconhecimento facial, desde que sigam as opiniões técnicas e recomendações que serão emitidas pela ANPD, e sigam os princípios norteadores da LGPD, no que se refere a proteção dos dados pessoais, até que uma lei especifica seja promulgada. Essa lei é essencial para que não se cumpra a preocupação do procurador Leonardo Roscoe Bessa exposta acima, de uma vigilância absoluta do Estado, como no romance "1984", de George Orwell.

A proteção de dados pessoais no Brasil e no mundo é uma realidade incontornável. Empresas e órgãos públicos devem se adaptar a essa nova realidade, pois esse é um caminho sem volta. Os dados pessoais do mundo inteiro circulam em uma rede mundial jamais vista em tamanho e conteúdo, e ainda, em constante expansão: a internet. Nunca foi tão importante essa proteção como é hoje. Há 30 anos, dificilmente um dado pessoal devidamente guardado seria vazado, contudo, hoje, um adolescente de 13 anos, de seu quarto na Austrália, é capaz de hackear dados de uma megaempresa como a Apple, nos Estados Unidos (Canaltech, 2019).

Tanta informação pessoal espalhada pode ser alvo de criminosos para cometer os mais diversos tipos de fraudes contra os titulares, ou até para influenciar a eleição presidencial do país mais poderoso do mundo, como foi o caso Facebook-Cambridge Analytica.

A proteção de dados pessoais deriva diretamente do direito à privacidade, no ponto em que o controle sobre seus dados é essencial para que sua vida privada não seja devassada por pessoas não autorizadas. Assim, as leis sobre proteção de dados pessoais são importantíssimas para assegurar o próprio direito à privacidade. Mas como garantir a proteção dos dados pessoais e o direito à privacidade sem frustrar o avanço tecnológico e o progresso em outras áreas do serviço público e privado, como a segurança? A resposta dessa pergunta é a chave para os avanços sociais futuros e o tema do capítulo a seguir.

4. O CONFLITO DE DIREITOS

Como já foi observado neste trabalho, tanto o direito à segurança como o direito à privacidade constituem direitos fundamentais na legislação brasileira e portuguesa. A situação exposta neste trabalho parece pôr em colisão esses dois direitos fundamentais, de um lado, o direito à segurança, efetivada por um sistema de reconhecimento facial capaz de melhor a segurança pública de uma região; e do outro lado, o direito à privacidade, direito individual de cada cidadão sobre sua imagem e dados biométricos, essencial para o desenvolvimento da personalidade humana.

Diante desse dilema, como deve ser resolvida essa matéria? Qual direito deve se sobrepor ao outro? O Estado pode utilizar tal tecnologia ou o direito à privacidade é suficiente para impedir a aplicação desse sistema?

Para responder a essas questões é importante se debruçar sobre o tema do conflito de direitos fundamentais e as formas de resolução.

4.1. Direitos fundamentais no Brasil

Os direitos fundamentais postulados na Constituição Federal brasileira possuem um forte conteúdo axiológico e são essenciais dentro do ordenamento jurídico, por isso possuem natureza de princípios (Maia, 2012).

Por ter um alto grau de abstração, os princípios permitem uma espécie de otimização, e se efetivam ao caso concreto na medida do possível. Existe uma liberdade, de forma que vários tipos de ação podem alcançar o mesmo objetivo final. Por outro lado, as regras possuem um baixo grau de abstração e são cumpridas exatamente como são previstas, não podem ser diminuídas, relativizadas ou afastadas por um momento. São aplicadas na fórmula do “tudo ou nada” (Hora, 2010).

As regras possuem uma narrativa mais objetiva e estão restritas às situações específicas às quais se dirigem. Já os princípios possuem um caráter mais abstrato e incidem sobre várias situações. Não existe hierarquia entre regras e princípios, devido ao princípio da unidade da Constituição (Barroso, 2003, apud Maia, 2012).

A classificação dos direitos fundamentais como regras ou princípios depende de interpretação, uma vez que esses direitos possuem uma estrutura flexível e complexa. Contudo, de acordo com Vale (2009, p. 129, apud Maia, 2012), “o forte conteúdo axiológico das normas de direitos fundamentais e sua elevada posição hierárquica no ordenamento jurídico fazem com que, na maioria das vezes, elas sejam interpretadas como princípios”.

Esses princípios podem ser considerados o centro do Direito Constitucional, e atualmente possuem a força de norma jurídica, superando o conceito de uma característica puramente axiológica e ética, sem eficácia jurídica ou aplicabilidade imediata e direta (Barroso, 2003, apud Maia, 2012).

Os direitos fundamentais podem ser classificados de acordo com a Teoria do status de Jellinek, onde esses direitos garantem aos indivíduos várias posições jurídicas em relação ao Estado. De acordo com essa teoria, os direitos fundamentais são divididos em três categorias: direitos de defesa, direitos prestacionais e direitos de participação (Maia, 2012).

Os direitos de defesa têm caráter negativo, eles exigem do Estado um dever de abstenção, no sentido de impedir a intromissão na autonomia dos indivíduos. São direitos que impõem limites ao poder estatal com o objetivo de resguardar as liberdades individuais (Novelino, 2008, apud Maia, 2012).

Os direitos prestacionais têm caráter positivo, compelindo o Estado a agir. Seu objetivo é que o poder público realize condutas ativas para proteger certos bens jurídicos de terceiros. Abrangem o direito a prestação matérias e jurídicas (Novelino, 2008, apud Maia, 2012).

Os direitos de participação, por sua vez, objetivam garantir que o cidadão participe na formação da vontade política da comunidade (Maia, 2012).

4.1.1. Relatividade dos direitos fundamentais

Os direitos fundamentais, enquanto princípios, possuem uma característica essencial, a sua relatividade. Como são princípios constitucionalmente previstos, os direitos fundamentais não são absolutos, diante de uma colisão entre eles haverá uma ponderação para se decidir qual o mais adequado (Maia, 2012).

Sobre a possibilidade de limitação dos direitos fundamentais, o Supremo Tribunal Federal (STF) definiu que, no sistema constitucional brasileiro, não existe direitos ou garantias que se revistam de caráter absoluto (Marmelstein, 2008, apud Maia, 2012).

E ainda, os direitos e garantias fundamentais consagrados na Constituição Federal brasileira não são ilimitados, visto que encontram seus limites nos demais direitos igualmente consagrados pela carta Magna (princípio da relatividade) (Morais, 2003, apud Maia, 2012).

Assim, verifica-se que os direitos fundamentais podem ser limitados por outros direitos fundamentais, devido à sua relatividade. O caráter não absoluto desses direitos faz com que,

diante de uma colisão, haja a avaliação de qual princípio mais adequado deve ser aplicado ao caso concreto.

4.1.2. Colisão entre direitos fundamentais no Brasil

Não é incomum direitos fundamentais colidirem. Em um Estado Democrático de Direito, a constituição costuma apresentar uma grande diversidade ideológica, de forma que as normas constitucionais podem vir a se apresentar de maneira potencialmente contraditórias. Assim, não são raras as vezes em que, no caso concreto, esses direitos entrem em rota de colisão (Marmelstein, 2008, apud Maia, 2012).

Existem muitos casos de colisão de direitos fundamentais, quando estes são postos em prática, como a liberdade de imprensa e o direito à privacidade, ou o direito à informação e o direito à intimidade.

Esses conflitos ocorrem em razão de ideologias conflitantes entre si, como o direito à informação e a liberdade de imprensa, que visam a transparência e a livre circulação da informação, contra os direitos de personalidade, que seguem o caminho do sigilo e da não exposição da vida privada (Maia, 2012).

Nesse momento de colisão, deve se chegar a uma solução de qual direito deve prevalecer em cada caso. Como já foi observado, os direitos fundamentais não possuem natureza absoluta, e diante da necessidade de se proteger um bem jurídico conflitante, também protegido constitucionalmente, isso pode justificar a restrição de um direito fundamental (Sarmento e Galdino, 2006, apud Maia, 2012).

E ainda, não existe hierarquia entre princípios, a precedência relativa de um sobre o outro deve ser definida diante de um caso concreto (Barroso, 2009, apud Maia, 2012).

Diante dessa ponderação de direitos fundamentais, aquele que irá decidir deve buscar a máxima otimização da norma, alcançando o máximo da vontade constitucional dos direitos conflitantes, sem sacrificar outros direitos igualmente protegidos (Marmelstein, 2008, apud Maia, 2012).

Mas esse discurso de direitos fundamentais não absolutos e sua relatividade diante de casos concretos pode levar a uma falsa noção de que esses princípios constitucionais são frágeis e podem ceder ante ao interesse público. Isso não é verdade. É importante ressaltar que a regra é o respeito aos direitos fundamentais, sendo sua restrição uma exceção (Marmelstein, 2008, apud Maia, 2012).

Assim, toda limitação de direitos fundamentais deve ser considerada potencialmente irregular, sendo indispensável uma ponderação entre direitos para se alcançar o resultado mais justo. Para isso, deve ser considerado o princípio da ponderação quando do exame da colisão de direitos fundamentais.

4.1.3. Princípio da ponderação e sua aplicação

O princípio da ponderação ou proporcionalidade é constituído de três pressupostos: adequação, necessidade e ponderação ou proporcionalidade em sentido estrito (Hora, 2010).

O pressuposto da adequação diz que medidas restritivas adotadas devem ser adequadas para alcançar os objetivos pretendidos. O requisito da necessidade prevê que a solução mais eficaz para se alcançar o objetivo a ser tomada seja a menos gravosa para os envolvidos (Costa, 2008). Assim, "apenas o que é adequado pode ser necessário, mas o que é necessário não pode ser inadequado" (Mendes, 1994, p. 475 apud Costa, 2008, p. 135).

Por fim, o pressuposto da ponderação ou da proporcionalidade em sentido estrito declara que os direitos fundamentais devem ser analisados dentro das circunstâncias em que se colidem, a fim de alcançar uma decisão aceitável, onde o direito limitado seja menos oneroso que o direito que se sobrepõe (Hora, 2010).

Essa é técnica de decisão (ponderação) que se emprega quando não é possível solucionar conflitos normativos através da hermenêutica, ou de critérios hierárquicos, cronológicos e de especialidade, que são os casos das colisões de normas constitucionais (Marmelstein, 2008, apud Maia, 2012).

Nesses casos, o intérprete deve se valer do princípio da concordância prática ou da harmonização, onde irá combinar os bens jurídicos em colisão, de forma a evitar o sacrifício total de um dos direitos. Ele deve realizar uma redução proporcional do alcance de cada um dos princípios em conflito, buscando os objetivos da norma constitucional e a sua harmonização (Morais, 2003, apud Maia, 2012).

Contudo, quando a harmonização se mostra inviável, o intérprete deve utilizar o sopesamento/ponderação como uma atividade intelectual para escolher qual direito deve predominar e qual deve ceder. Esse é o grande transtorno da ponderação, é inevitável o descumprimento total ou parcial de alguma norma constitucional. Nesse momento, o juiz deve tomar uma difícil decisão, julgar qual dos princípios constitucionais "vale menos" para ser sacrificado no caso concreto (Marmelstein, 2008, apud Maia, 2012).

Assim, sempre que houver o conflito de normas constitucionais, o legislador ou o juiz, deve buscar a solução através da harmonização dos direitos, fazendo com que seus limites sejam ajustados e cada princípio possa ser aproveitado ao máximo, dentro da limitação imposta pelo outro direito em conflito, para aquele caso. Caso não seja possível a harmonização, deve ser feita a ponderação com o intuito de sacrificar o mínimo possível o direito que deve ceder no caso analisado.

4.2. Direitos Fundamentais em Portugal

A CRP traz uma série de direitos fundamentais, mas esses direitos não se limitam ao texto constitucional. Portugal também acolhe fontes extraconstitucionais de direitos fundamentais, como a Declaração Universal dos Direitos Humanos (DUDH) (Gouveia, 2018).

Nesse sentido, a Carta também traz possibilidades de limitação ao exercício dos direitos fundamentais dentro do sistema constitucional português. Em seu art. 29º, nº 2, a DUDH apresenta uma cláusula geral de restrição, que diz: "no exercício deste direito e no gozo destas liberdades ninguém está sujeito senão às limitações estabelecidas pela lei com vista exclusivamente a promover o reconhecimento e o respeito dos direitos e liberdades dos outros e a fim de satisfazer as justas exigências da moral, da ordem pública e do bem-estar numa sociedade democrática".

Apesar de ainda controverso na doutrina portuguesa, quanto à aceitação da aplicação dessa cláusula limitadora dos direitos fundamentais no direito português, o professor Jorge Bacelar Gouveia (2018) ensina que, diante da lacuna constitucional da CRP, referente a essa matéria, e ainda, tendo em conta a vertente integrativa da CRP à DUDH, é legítima a aplicação desse artigo no regime constitucional de direitos fundamentais.

A DUDH apresenta uma justificativa relevante para a limitação ao exercício de direitos fundamentais, a "ordem pública". Mas essa não é uma aplicação indiscriminada nem arbitrária, ela exige um contexto de Estado Democrático. Assim, a invocação da ordem pública para a limitação de direitos fundamentais exige o referido contexto. E ainda, não se trata da ordem pública no sentido restrito da segurança interna, mas sim, em sentido amplo, invocada para defender a segurança nacional, voltada para a segurança externa e de Estado (Gouveia, 2018).

4.2.1. Colisão de direitos fundamentais em Portugal

Para a solução da colisão de direitos fundamentais em Portugal, duas possibilidades podem ser utilizadas (Gouveia, 2018):

1. A cláusula geral do art. 29º, nº 2, da DUDH;
2. A cláusula geral do art. 335º do Código Civil[7].

Em ambos os casos, a matéria "segurança" é importante para determinar a limitação externa de direitos fundamentais em uma colisão de direitos.

Na primeira hipótese, a DUDH aponta para a colisão do direito à segurança com a necessidade de os indivíduos suportarem "…limitações estabelecidas pela lei com vista exclusivamente a promover o reconhecimento e o respeito dos direitos e liberdades dos outros…" (Gouveia, 2018, p. 356).

Os direitos fundamentais não são ilimitados, e encaram limites ao seu exercício ante a leis que os restrinja com a finalidade de proteger o exercício do direito à segurança por parte de outros cidadãos. A "segurança", direto fundamental previsto na DUDH, se apresenta como uma situação jurídica limitadora de outros direitos (Gouveia, 2018).

Na segunda hipótese, o Código Civil Português apresenta soluções para a colisão de direitos subjetivos. Sendo o direito à segurança um direito subjetivo fundamental, ele pode colidir com outros direitos, requerendo a sua solução por intermédio desse artigo(Gouveia, 2018).

4.2.2. Direitos absolutos x direito à segurança

É comum a doutrina argumentar que os direitos fundamentais absolutos – os que nem o estado de exceção pode tolher – estão em um patamar superior na ordem jurídica, prevalecendo sobre qualquer outro direito com os quais entre em conflito (Gouveia, 2018).

Essa é uma visão hierarquizante, onde a solução da colisão de direitos fundamentais seria solucionada por uma tabela fixa. Contudo, essa não é uma teoria convincente, pois a solução do conflito de direitos não pode partir de uma ordem hierarquizada dos valores

[7] PORTUGAL. Código Civil, Art. 335º (Colisão de direitos) – 1. Havendo colisão de direitos iguais ou da mesma espécie, devem os titulares ceder na medida do necessário para que todos produzam igualmente o seu efeito, sem maior detrimento para qualquer das partes. 2. Se os direitos forem desiguais ou de espécie diferente, prevalece o que deva considerar-se superior.

constitucionais (Andrade, 2009, p. 321 apud Gouveia, 2018, p. 357). Antes, deve ser procedida uma apreciação concreta, de acordo com a teoria da ponderação dos bens. Somente assim, o intérprete estaria habilitado a decidir, devendo primeiro efetuar a harmonização e, não sendo possível essa, aplicar uma orientação de prevalência (Canotilho, 2003, pp. 646 e 647 apud Gouveia, 2018, p. 358).

É utópico pensar a solução da colisão de direitos com base em uma tabela fixa e hierarquizada, pois não apenas está fora da realidade como nem sequer resolve conflitos de diretos hierarquicamente iguais. Essa não é uma solução constitucionalmente adequada (Gouveia, 2018).

Apesar disso, o conceito de direito fundamental absoluto, como é o caso da dignidade da pessoa humana, pode ser útil quando não é possível a harmonização de direitos, e a ponderação concreta de bens exige a prevalência de um direito sobre o outro. Nesse sentido, os direitos absolutos auxiliam a decisão do interprete no momento de julgá-los mais relevantes que outros direitos em colisão, determinando a sua prevalência (Gouveia, 2018).

Entretanto, ainda que os direitos fundamentais absolutos tenham a sua relevância perante outros direitos, eles não são insuperáveis. Mais uma vez, os direitos não podem estar dispostos em uma prateleira hierarquizada, rígida e abstrata. Diante de exigências concretas, o direito à segurança pode prevalecer até sobre direitos fundamentais absolutos (Gouveia, 2018).

4.3. O direito à privacidade impede o emprego da tecnologia de reconhecimento facial na segurança pública?

A resposta a essa pergunta soluciona o problema apresentado na introdução desta dissertação de mestrado e, provavelmente, para aqueles que nos acompanharam até aqui, já devem ter a resposta em suas mentes. Sem delongas, a resposta é “não”. O direito à privacidade não impede o emprego da tecnologia de reconhecimento facial na segurança pública.

Isso porque, como ficou demonstrado nos tópicos anteriores, nenhum direito é absoluto, ou hierarquicamente superior, em relação aos demais direitos. Mesmo o direito à vida, direito fundamental protegido constitucionalmente no Brasil, inclusive com vedação

constitucional da pena de morte[8], pode ser suprimido em tempos de guerra, como no crime de traição[9].

Para que um direito prevaleça sobre o outro, deve ser feita uma ponderação dos direitos, para o caso concreto. Assim, será possível estabelecer se a harmonização dos direitos soluciona o problema apresentado, alterando os limites de cada direito para que os dois possam ser cumpridos no máximo possível; ou se será necessário que um direito prevaleça sobre o outro, por vezes suprimindo completamente o outro direito, como no caso de traição em tempo de guerra.

Essa ponderação para solução da colisão de direitos pode ser feita tanto pelo juiz, analisando um caso concreto que lhe foi apresentado após um choque real de direitos, como em um caso de liberdade de imprensa *versus* direito à privacidade. Como também pelo legislador, que diante de uma realidade social atual ou futura, pode criar uma lei para harmonizar esses direitos.

Foi precisamente o que aconteceu através das legislações apresentadas no capítulo anterior. Se essa pesquisa acadêmica tive sido realizada em 2017, no Brasil, ou em 2015 em relação à Europa, a discussão possivelmente seria sobre a criação de uma legislação para regulamentar esse conflito de direitos.

Contudo, em 2019, esse não é mais o problema. Atualmente, com a recém aprovada, apesar de ainda não estar em vigor, Lei Geral de Proteção de Dados no Brasil, e com o Regulamento Geral de Proteção de Dados, juntamente com a Diretiva (UE) 2016/680, ambos em vigor na União Europeia, a antiga lacuna legislativa já não existe para Brasil e Portugal.

Inclusive, em relação à ponderação de direitos, são objetivos dessas legislações a harmonização dos direitos fundamentais com outros direitos em colisão.

Como pode ser observado na justificativa do Projeto de Lei nº. 4060/2012, que deu origem à LGPD do Brasil, onde o então Deputado Federal Milton Monti expõe que o projeto de lei "…tem por objetivo dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como a proteção dos direitos individuais das pessoas…". E ainda, dentro da

[8] BRASIL. Constituição da República Federativa do Brasil de 1988, art. 5º, XLVII - não haverá penas: a) de morte, salvo em caso de guerra declarada, nos termos do art. 84, XIX;
[9] BRASIL. Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar. Traição: Art. 355. Tomar o nacional armas contra o Brasil ou Estado aliado, ou prestar serviço nas forças armadas de nação em guerra contra o Brasil: Pena - morte, grau máximo; reclusão, de vinte anos, grau mínimo.

realidade dos avanços tecnológicos da informação e sua relação com os indivíduos, ressalta que "…se faz necessário estabelecer normas legais para disciplinar tais relações, especialmente para dar proteção à individualidade e a privacidade das pessoas, sem impedir a livre iniciativa comercial e de comunicação".

Perceba que o objetivo da lei é regulamentar o tratamento de dados pessoais, incluindo os dados biométricos captados por câmeras de reconhecimento facial, e proteger os direitos individuais dos cidadãos, inclusive o direito à privacidade, sem que isso impeça a livre iniciativa comercial e de comunicação. Ou seja, a lei visa harmonizar a proteção dos direitos individuais com a livre iniciativa comercial e de comunicação.

Isso também pode ser observado no RGPD da União Europeia, que em seu considerando nº 3 relata que o Regulamento "…visa *harmonizar* a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros".

Note que o RGPD inclusive utiliza o termo "harmonizar", quando cita que a sua finalidade é a harmonia entre a defesa dos direitos e liberdades fundamentais, como o direito à privacidade, e a livre circulação de dados pessoais. Mais uma vez, fica claro que o objetivo não é restringir nem os direitos fundamentais, nem a livre circulação de dados, que já ocorre mundialmente através da internet, mas antes, conciliar pacificamente a convivência desses direitos.

Por fim, a Diretiva (UE) 2016/680, também, reforça essa ideia, quando expõe, em seu considerando nº 15, que "a fim de assegurar o mesmo nível de proteção para as pessoas singulares através de direitos suscetíveis de proteção judicial no conjunto da União e evitar divergências que criem obstáculos ao intercâmbio de dados pessoais entre as autoridades competentes, a presente diretiva deverá prever regras *harmonizadas* para a proteção e a livre circulação de dados pessoais tratados para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais […]".

Aqui, com o objetivo de assegurar a proteção dos direitos individuais sem que isso atrapalhe o intercâmbio de informação entre autoridades competentes, a Diretiva prevê regras *harmonizadas* entre a proteção e a livre circulação de dados pessoais tratados para o fim exclusivo da diretiva. Seguindo os passos do RGPD, a Diretiva também busca a harmonização de direitos, onde cada um cede o suficiente para que ambos sejam cumpridos no limite máximo possível do caso estudado.

Além disso, diante do caso concreto, pode se expor mais justificativas para a implementação da tecnologia do reconhecimento facial na segurança pública. O Brasil, por

exemplo, possui números assustadores de violência, que foram apresentados no primeiro capítulo. Números que nos fazem crer, muitas vezes, que o país vive uma guerra civil.

Nesse sentido, quanto mais ferramentas o país tiver para combater os altos índices criminais, maior será a sua efetividade. Em momentos em que se pede que o Estado faça mais com menos, ferramentas tecnológicas auxiliam as forças de segurança no combate à criminalidade, sem ter que recorrer ao constante aumento de efetivo e compra de viaturas, que aumentam demasiadamente o gasto orçamentário.

Nesse conflito entre a segurança coletiva e a proteção do direito individual de privacidade do cidadão, deve se alcançar um meio termo que seja melhor para todos. Como foi exposto no capítulo anterior, o direito à segurança é um direito que estabelece um estado de proteção que possibilita aos cidadãos o gozo de todos os demais direitos individuais e coletivos (Fabretti, 2014).

Assim, é de suma importância garantir o direito à segurança, pois isso possibilita, inclusive, a proteção do próprio direito à privacidade. Em uma sociedade em que o direito à segurança não é minimamente garantido, todos os outros direitos fundamentais estão passíveis de serem feridos. Como explica Gouveia (2018, p. 299), o direito à segurança tem a função de "direito fundamental sobreposto", onde o seu objeto se torna a soma dos objetos específicos de cada um dos outros direitos fundamentais.

O clamor por segurança no Brasil, embasado nessa vital necessidade de se garantir esse direito, aliado à efetividade do sistema de câmeras com a tecnologia de reconhecimento facial, são suficientes para se implantar essa medida de forma harmonizada com o direito à privacidade, através do fiel cumprimento da atual legislação apresentada, que é adequada para se fazer cumprir esses direitos dentro um limite eficaz para todos.

4.3.1. Diretiva (UE) 2016/680 e a LGPD na harmonização dos direitos

Como foi explanado no capítulo anterior, as legislações atuais de Brasil e Portugal não impedem a implementação da tecnologia de reconhecimento facial através de câmeras pelos órgãos de segurança pública.

No Brasil, porque a própria LGPD não se aplica quando o tratamento de dados tem o fim exclusivo de segurança pública, ficando subordinado às opiniões técnicas e recomendações da ANPD. E em Portugal, porque tanto a Diretiva (UE) 2016/680, que regulamenta como o tratamento de dados pessoais deve ser feito pelos órgãos de segurança pública – que será transposta em breve –, como também a Lei nº 1/2005, que regula a

utilização de câmeras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, têm o objetivo de estabelecer normas de como deve ser utilizada tais tecnologias, e não o viés de as proibir.

Isso pode ser observado ao longo de toda a legislação que foi estudada nesse trabalho. Tanto a Diretiva (UE) 2016/680 quanto a LGPD, ambas derivadas do RGPD, estabelecem uma série de normas para se proteger os direitos e garantias individuais do cidadão.

Isso fica claro quando a Diretiva (UE) 2016/680, no art. 4º, e a LGPD, no art. 6º, declaram um rol de princípios norteadores de tratamento dos dados pessoais, os quais garantem que os mesmos sejam tratados dentro da legalidade, necessidade, adequabilidade, transparência, segurança, dentre outros princípios.

Além disso, essas leis trazem um capítulo próprio para tratar dos direitos do titular dos dados. O capitulo III, de ambas as legislações, explica quais direitos o titular dos dados possui frente àqueles que tratam dos seus dados. Isso vem para balancear o poder entre as partes, uma vez que o titular está em uma posição fragilizada em relação à autoridade competente para tratar os dados pessoais.

Nesse sentido, a Diretiva (UE) 2016/680 traz direitos como o de saber a identidade do responsável pelo tratamento, saber a finalidade da coleta, de solicitar o acesso de seus dados pessoais, de requerer a sua retificação, o seu apagamento e a limitação do tratamento, dentre outros direitos.

Já a LGPD deixa assegurado que a titularidade dos dados pessoais é de cada pessoa natural, sendo-lhes garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Além disso, ao longo do capítulo, pontua os vários direitos do titular, como acesso aos dados, bloqueio ou eliminação de dados desnecessários, excessivos, ou tratados em desconformidade com o disposto na lei, revogação de consentimento, dentro outros.

Cabe ressaltar, mais uma vez, que a LGPD não é uma lei especifica para os órgãos de segurança pública, como é a Diretiva (UE) 2016/680. Assim, esses direitos são gerais para todos aqueles que tratam dados pessoais, até que seja sancionada uma lei específica para o tratamento de dados pessoais pelas forças de segurança, ou a ANPD emita opiniões técnicas ou recomendações referentes a esse tema.

Seja em termos gerais, quando se expõe o conflito de direitos referente ao tema apresentado, seja em termos específicos, quando se analisa a legislação pertinente à matéria, a proteção das liberdades e garantias fundamentais, como o direito à privacidade, não impedem a implementação da tecnologia de reconhecimento facial pelos órgãos da segurança pública no Brasil ou em Portugal.

Ao contrário, diante da análise dessas leis, percebe-se que a ideia é justamente pavimentar o caminho para a implementação de inovações tecnológicas, ao mesmo tempo em que se garante a proteção dos direitos fundamentais. Se trata de uma evolução legislativa inevitável, pois não se pode frenar os avanços tecnológicos, principalmente, os que vêm para melhorar a vida dos cidadãos, ao passo que, também, não se pode deixar livre de regulamentação todas as tecnologias que aparecem no mercado, sob pena de se ferir gravemente, e as vezes irreversivelmente, direitos e garantias fundamentais. A solução é criar leis que harmonizem esses princípios, como as que foram apresentadas nesse trabalho, a fim de se ter um ambiente social livre, seguro e desenvolvido.

CONCLUSÃO

A atual sociedade da informação tem vivido uma fase de avanços tecnológicos sem precedentes. Hoje, o dado pessoal é um produto que gera valor para as pequenas e grandes corporações, desde dados sobre sua saúde, que auxiliam em diagnósticos médicos, até dados sobre seu perfil e suas preferências pessoais, para buscar seu par romântico ideal. E esses dados circulam o mundo em uma rede jamais vista em tamanho e conteúdo, e ainda, em constante expansão: a internet.

Nesse cenário, é essencial a proteção desses dados pessoais, pois esse direito deriva diretamente do direito fundamental à privacidade, que por sua vez, é indispensável para o desenvolvimento da personalidade individual e para se garantir a dignidade da pessoa humana.

Do outro lado, se tem o direito à segurança, direito fundamental importantíssimo dentro de uma sociedade, pois ele garante um cenário de ordem e proteção para que todos os outros direitos fundamentais possam ser gozados. Assim, o direito à segurança adquire a função de "direito fundamental sobreposto", onde o seu objeto se torna a soma dos objetos específicos de cada um dos outros direitos fundamentais.

O tema estudado nessa dissertação põe em confronto justamente estes dois direitos fundamentais: avanços tecnológicos que trazem uma poderosa ferramenta no combate à criminalidade (direito à segurança), que nesse caso é a tecnologia do reconhecimento facial, mas que, inevitavelmente, adentram a esfera privada do cidadão, uma vez que capturam a sua imagem/dados biométricos e realizam o tratamento de dados pessoais (direito à privacidade).

Esse choque não é uma novidade, e ainda vai acontecer várias vezes ao longo da jornada da humanidade. O binômio tecnologia-privacidade anda junto, e quando se tenta fortalecer um dos lados, o outro lado protesta para não se ver extinto ou obsoleto. O desafio é promover o avanço tecnológico para o incremento da qualidade de vida sem ofender os direitos fundamentais do ser humano.

Nesse quadro, o Estado tem um papel fundamental, ele que vai equilibrar a proteção dos direitos fundamentais e o livre desenvolvimento tecnológico. Como foi observado, uma das principais razões do Estado é garantir a segurança do seu povo em um determinado território, para que esse possa se desenvolver em uma organização social complexa.

Assim, o Estado deve buscar garantir a segurança, dentro dos meios que estão disponíveis, sem que isso ofenda os demais direitos fundamentais. Nessa tentativa, por

vezes, alguns direitos fundamentais podem entrar em rota de colisão. A solução da colisão de direitos é uma tarefa complexa, e exige um julgamento preciso, de acordo com o contexto em análise.

Como foi observado, nenhum direito é absoluto, no sentido de se sobrepor, automaticamente, a qualquer outro direito. Nenhum direito é ilimitado, pois seus limites são impostos pelos demais direitos igualmente consagrados na constituição.

A relatividade dos direitos fundamentais mostra que, dentro de um contexto factual, qualquer direito pode ser limitado ou sobreposto por outro direito. Quando dois direitos fundamentais se colidem, como no caso apresentado neste trabalho, o poder judiciário, ou o legislativo, deve realizar os seguintes passos para se alcançar a decisão mais justa para o caso concreto: a harmonização, e, não sendo possível essa, a ponderação dos direitos.

Assim, sempre que houver o conflito de normas constitucionais, o legislador ou o juiz, deve buscar a solução através da harmonização dos direitos, fazendo com que seus limites sejam ajustados e cada direito possa ser aproveitado ao máximo, dentro da limitação imposta pelo outro direito em conflito, para aquele caso. Caso não seja possível a harmonização, deve ser feita a ponderação com o intuito de sacrificar o mínimo possível o direito que deve ceder no caso analisado.

Através do estudo da legislação do Brasil e de Portugal – principalmente da Lei Geral de Proteção de Dados (Lei nº 13.709/18, alterada pela Lei nº 13.853/19), para o Brasil, e do Regulamento Geral de Proteção de Dados, juntamente com a Diretiva (UE) 2016/680, para Portugal –, foi possível se chegar à resposta da pergunta que orientou essa dissertação: O direito à privacidade impede o emprego da tecnologia de reconhecimento facial na segurança pública? A resposta é “não”.

O direito à privacidade não impede o emprego da tecnologia de reconhecimento facial na segurança pública. Evidentemente, que essa é a resposta para o contexto analisado, ou seja, para Brasil e Portugal na realidade atual.

Isso porque, as leis citadas acima vieram, justamente, para harmonizar o conflito de direitos existente quando do tratamento de dados pessoais através das mais diversas tecnologias, dentre elas, o reconhecimento facial.

O objetivo dessas leis foi garantir a proteção dos direitos e liberdades fundamentais, como o direito à privacidade, sem que isso viesse a impedir a livre circulação de dados pessoais ou a livre iniciativa comercial e de comunicação. Ou seja, essas leis vieram para proteger o cidadão e permitir os avanços tecnológicos; garantir os direitos fundamentais do

indivíduo e possibilitar o desenvolvimento de empresas; proteger o direto à privacidade e viabilizar o emprego de novas tecnologias, pelo Estado, na defesa do cidadão.

Essas leis vieram para harmonizar direitos, garantir que esses direitos, em um cenário de conflito, possam coexistir, e serem protegidos e respeitados, até um limite que não impeça o exercício do outro direito.

Portanto, verifica-se que as legislações, do Brasil e de Portugal, estão alinhada com a atual evolução da sociedade da informação, que diariamente cria inovações tecnológicas para melhorar a vida humana, porém, necessita de uma regulação estatal precisa, sendo, ao mesmo tempo, leve, para não impedir progresso científico, e contundente, para proteger os direitos e garantias fundamentais de seus cidadãos.

BIBLIOGRAFIA

AIETA, Vânia Siciliano - **A garantia da intimidade como direito fundamental**. Rio de Janeiro : Lumen Juris, 1999

ALECRIM, Emerson - **Tecnoblog - Tecnologia do Facebook pode identificar rostos quase tão bem quanto você** [Em linha], atual. 2014. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:https://tecnoblog.net/153371/tecnologia-facebook-identificar-rostos/>.

ALVES, Raoni - **PM vai ampliar os testes com as câmeras de reconhecimento facial no Rio** [Em linha], atual. 2019. [Consult. 7 mar. 2019]. Disponível em WWW:<URL:https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/03/22/pm-vai-ampliar-os-testes-com-as-cameras-de-reconhecimento-facial-no-rio.ghtml>.

ARAÚJO, José Laércio Da Silva - **Intimidade, vida privada e direito penal**. São Paulo : Madras, 2000

ARAÚJO, Marcos Elias Cláudio De; PASQUALI, Luiz - **Histórico dos processos de identificação** [Em linha] [Consult. 1 fev. 2019]. Disponível em WWW:<URL:http://www.institutodeidentificacao.pr.gov.br/arquivos/File/forum/historico_processos.pdf>.

ASSEMBLEIA DA REPÚBLICA - **Proposta de Lei 125/XIII** [Em linha], atual. 2018. [Consult. 3 jul. 2019]. Disponível em WWW:<URL:https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42505>.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra Da Silva - **Comentários à Constituição do Brasil**. São Paulo : Saraiva, 1989

BBC - **G1 - Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades** [Em linha], atual. 2018. [Consult. 8 jul. 2019]. Disponível em WWW:<URL:https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>.

BBC NEWS - **Como funciona o 'Big Brother' da China, com 170 milhões de câmeras que fazem identificação visual** [Em linha], atual. 2017. [Consult. 27 mar. 2019]. Disponível em WWW:<URL:https://www.bbc.com/portuguese/internacional-42361047>.

BBC NEWS - **Chinese man caught by facial recognition at pop concert** [Em linha], atual. 2018. [Consult. 25 mar. 2019]. Disponível em WWW:<URL:https://www.bbc.com/news/world-asia-china-43751276>.

BONSOR, Kevin; JOHNSON, Ryan - **How Facial Recognition Systems Work** [Em linha], atual. 2001. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>.

BORGES, Liliana - **Público.pt - Washington classifica Portugal como um dos países mais seguros do mundo** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:https://www.publico.pt/2018/01/22/mundo/noticia/eua-classificam-portugal-como-um-dos-destinos-mais-seguros-do-mundo-1800263>.

BUMP, Pamela - **Facial Recognition in Law Enforcement – 6 Current Applications / EMERJ** [Em linha], atual. 2018. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:https://emerj.com/ai-sector-overviews/facial-recognition-in-law-enforcement/>.

CANALTECH - **Hacker adolescente que invadiu servidores da Apple não será preso** [Em linha], atual. 2019. [Consult. 11 jul. 2019]. Disponível em WWW:<URL:https://canaltech.com.br/hacker/hacker-adolescente-que-invadiu-servidores-da-apple-nao-sera-preso-140199/>.

CAPUCHO, Joana - **Na polícia, no carro, no aeroporto, o reconhecimento facial já não é ficção** [Em linha], atual. 2018. [Consult. 27 mar. 2019]. Disponível em WWW:<URL:https://www.dn.pt/sociedade/interior/na-policia-no-carro-no-aeroporto-o-reconhecimento-facial-ja-nao-e-ficcao-9047999.html>.

CENTRAL CFTV - **centralcftv** [Em linha], atual. 2019. [Consult. 15 mar. 2019]. Disponível em WWW:<URL:http://www.centralcftv.com/>.

CHINA DAILY - **Facial recognition in Jiangsu train stations nets 137 fugitives** [Em linha], atual. 2018. [Consult. 25 mar. 2019]. Disponível em WWW:<URL:http://www.chinadaily.com.cn/a/201808/08/WS5b6a52f8a310add14f38494e.html>.

CNPD - **Comunicado da CNPD - Aplicação do novo quadro legal de proteção de dados** [Em linha], atual. 2018. [Consult. 3 jul. 2019]. Disponível em WWW:<URL:https://dre.pt/documents/10184/826042/Comunicacao+CNPD_25_5_2018.pdf/87e28703-4e8c-4439-9ba9-f0f7b75ceab1>.

CNPD - **História da CNPD** [Em linha], atual. 2019. [Consult. 8 jul. 2019]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/cnpd/historia.htm>.

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS - **O que é a CNPD?** [Em linha], atual. 2019. [Consult. 8 jul. 2019]. Disponível em WWW:<URL:https://www.cnpd.pt/bin/cnpd/acnpd.htm>.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA - **Retratos da sociedade brasileira**. Brasília : CNI, 2018, atual. 2018.

CONJUR - **IDP debate perspectivas regulatórias para o reconhecimento facial** [Em linha], atual. 2019. [Consult. 8 jul. 2019]. Disponível em WWW:<URL:https://www.conjur.com.br/2019-mai-06/idp-debate-perspectivas-regulatorias-reconhecimento-facial>.

CORREIA, Victor - Sobre o direito à privacidade. Em MIRANDA, JORGE (Ed.) - **Revista: O Direito - Ano 146º - I**. Lisboa : Almedina, 2014

CORUM, Chris - **London facial recognition test nabs suspects via video surveillance** [Em linha], atual. 2019. [Consult. 27 mar. 2019]. Disponível em WWW:<URL:https://www.secureidnews.com/news-item/london-facial-recognition-test-nabs-suspects-via-video-surveillance/>.

COSTA, Alexandre Araújo - **O Controle de Razoabilidade no Direito Comparado**. Brasília : Thesaurus, 2008

COUTELLE, José Eduardo - **Qual a porcentagem de crimes solucionados pela polícia no Brasil? - Superinteressante** [Em linha], atual. 2018. [Consult. 15 fev. 2019]. Disponível em WWW:<URL:https://super.abril.com.br/mundo-estranho/qual-a-porcentagem-de-crimes-solucionados-pela-policia-no-brasil/>.

CUOMO, Andrew M. - **Governor Cuomo Announces Major Facial Recognition Technology Milestone with 21,000 Fraud Cases Investigated** [Em linha], atual. 2017. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:https://www.governor.ny.gov/news/governor-cuomo-announces-major-facial-recognition-technology-milestone-21000-fraud-cases>.

CUTHBERTSON, Anthony - **Indian Police trace 3,000 missing children in just four days using facial recognition technology** [Em linha], atual. 2018. [Consult. 27 mar. 2019]. Disponível em WWW:<URL:https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html>.

DAVIES, Bethan; DAWSON, Andrew; INNES, Martin - **How facial recognition technology aids police** [Em linha], atual. 2018. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:https://phys.org/news/2018-11-facial-recognition-technology-aids-police.html>.

DEBORD, Guy - **A Sociedade do Espetáculo**. São Paulo : eBooksBrasil.com, 2003

DELEUZE, Gilles - **Conversações**. São Paulo : 34, 1992

DEURSEN, Felipe Van - **Superinteressante - O Brasil tem mais assassinatos do que todos estes países somados** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:https://super.abril.com.br/blog/contaoutra/o-brasil-tem-mais-assassinatos-do-que-todos-estes-paises-somados/>.

DEVFUN LAB - **The Future of Face Recognition** [Em linha], atual. 2017. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:http://devfun-lab.com/1214>.

DIÁRIO DE NOTÍCIAS - **«Foi o terrorismo que desenvolveu esta técnica»** [Em linha], atual. 2018. [Consult. 27 mar. 2019]. Disponível em WWW:<URL:https://www.dn.pt/sociedade/interior/foi-o-terrorismo-que-desenvolveu-esta-tecnica-9048005.html>.

DONEDA, Danilo - **Da privacidade à proteção de dados pessoais**. Rio de Janeiro : Renovar, 2006

ECO - **Portugal no top dos países mais seguros do mundo. Islândia lidera há 11 anos** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:https://eco.sapo.pt/2018/06/28/portugal-e-o-quarto-pais-mais-seguro-do-mundo-islandia-lidera-lista-ha-11-anos/>.

EUROPA.EU - **Regulamentos, diretivas e outros atos legislativos** [Em linha], atual. 2019. [Consult. 8 jul. 2019]. Disponível em WWW:<URL:https://europa.eu/european-union/eu-law/legal-acts_pt>.

EUROPEAN COMMISSION - **Data Protection Law Enforcement Directive (EU) 2016/680 transposition - Updated State of play in the Member States (12/04/2019)** [Em linha], atual. 2019. [Consult. 3 jul. 2019]. Disponível em

WWW:<URL:http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=30309>.

FABRETTI, Humberto Barrionuevo - **Segurança Pública: Fundamentos jurídicos para uma abordagem constitucional**. São Paulo : Atlas, 2014

FACEFIRST - **Transform Law Enforcment with Face Recognition** [Em linha], atual. 2013. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:https://www.facefirst.com/wp-content/uploads/2017/07/Law_Enforcement_One_Sheet.pdf>.

FALA BRASIL - **Saiba como funciona o reconhecimento facial que começa a ser usado em prédios e aeroportos - Youtube** [Em linha], atual. 2017. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:https://www.youtube.com/watch?v=6IUZ0qM5kj0>.

FBSP - **Segurança Pública em Números - Anuário Brasileiro de Segurança Pública 2018** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:http://www.forumseguranca.org.br/wp-content/uploads/2018/08/Apresentação_Anuário.pdf>.

FOUCAULT, Michel - **Vigiar e Punir**. Rio de Janeiro : Vozes, 1999

FROIS, Catarina - **A Sociedade Vigilante - ensaios sobre identificação, vigilância e privacidade**. Lisboa : ICS, 2008

G1-GLOBO - **Brasil chega à taxa de 30 assassinatos por 100 mil habitantes em 2016, 30 vezes a da Europa, diz Atlas da Violência** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:https://g1.globo.com/sp/sao-paulo/noticia/brasil-chega-a-taxa-de-30-assassinatos-por-100-mil-habitantes-em-2016-30-vezes-a-da-europa-diz-atlas-da-violencia.ghtml>.

G1 RIO - **Polícia Militar vai utilizar câmeras de reconhecimento facial na final da Copa América** [Em linha], atual. 2019. [Consult. 11 jul. 2019]. Disponível em WWW:<URL:https://g1.globo.com/google/amp/rj/rio-de-janeiro/noticia/2019/07/05/policia-militar-vai-utilizar-cameras-de-reconhecimento-facial-na-final-da-copa-america.ghtml?__twitter_impression=true>.

GAMIZ, Mario Sergio De Freitas - **Privacidade e Intimidade: doutrina e jurisprudência**. Curitiba : Juruá, 2012

GARCIA, José Luís - A automobilização da ciência para a criação de aparelhos de identificação e de coacção estatal em finais do século XIX. **A Sociedade Vigilante - ensaios sobre identificação, vigilância e privacidade**. 2008) 43–64.

GLOBOPLAY - **Câmeras de reconhecimento facial ajudam a polícia a encontrar criminosos** [Em linha], atual. 2019. [Consult. 11 jul. 2019]. Disponível em WWW:<URL:https://globoplay.globo.com/v/7444804/>.

GOUVEIA, Jorge Bacelar - **Direito da Segurança. Cidadania, Soberania e Cosmopolitismo**. Coimbra : Almedina, 2018

HEMPEL, Leon; TÖPFER, Eric - **Urban Eye: Inception Report to the European Commission, 5th Framework Programme** [Em linha], atual. 2002. [Consult. 2 mar. 2019]. Disponível em WWW:<URL:http://www.urbaneye.net/results/ue_wp1.pdf>.

HEMPEL, Leon; TÖPFER, Eric - **CCTV in Europe - Final report** [Em linha], atual. 2004. [Consult. 2 mar. 2019]. Disponível em WWW:<URL:http://www.urbaneye.net/results/ue_wp15.pdf>.

HOBBES, Thomas - **Leviatã**. São Paulo : Martins Fontes, 2003

HORA, Carolina Prado Da - **A resolução dos conflitos de direitos fundamentais** [Em linha], atual. 2010. [Consult. 22 jul. 2019]. Disponível em WWW:<URL:https://ambitojuridico.com.br/cadernos/direito-constitucional/a-resolucao-dos-conflitos-de-direitos-fundamentais/>.

INSTITUTE FOR ECONOMICS & PEACE - **Global Peace Index 2018: Measuring Peace in a Complex World** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:http://visionofhumanity.org/app/uploads/2018/06/Global-Peace-Index-2018-2.pdf>.

INSTITUTE FOR ECONOMICS & PEACE - **GLOBAL PEACE INDEX 2018 SNAPSHOT** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:http://visionofhumanity.org/app/uploads/2018/06/Global-Peace-Index-2018-Snapshot.pdf>.

JABUR, Gilberto Haddad - **Liberdade de pensamento e direito à vida privada: conflito entre direitos da personalidade**. São Paulo : Revista dos Tribunais, 2000

JORNAL DA USP - **Números da violência no Brasil já equivalem aos de um país em guerra** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:https://jornal.usp.br/atualidades/numeros-da-violencia-no-brasil-ja-equivalem-aos-de-um-pais-em-guerra/>.

KAFKA, Franz - **O Processo**. Alfragide : Dom Quixote, 2009

LIU, Joyce; XIQING, Wang - **In Your Face: China's all-seeing state** [Em linha], atual. 2017. [Consult. 25 mar. 2019]. Disponível em WWW:<URL:https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state>.

LOCKE, John - **Dois Tratados Sobre o Governo**. São Paulo : Martins Fontes, 1998

LOPES, Ana Isabel; SANTOS, Sónia - **Da Sociedade disciplinar à Sociedade de Controle** [Em linha], atual. 2002. [Consult. 11 fev. 2019]. Disponível em WWW:<URL:http://www.educ.fc.ul.pt/docentes/opombo/hfe/momentos/sociedade disciplinar/index.htm>.

LUNARDI, Soraya Gasparetto - **Direito à segurança e segurança pública - na perspectiva da Constituição brasileira de 1988** [Em linha] [Consult. 24 mai. 2019]. Disponível em WWW:<URL:https://www.academia.edu/37456463/DIREITO_À_SEGURANÇA_E_SEGURANÇA_PÚBLICA_-NA_PERSPECTIVA_DA_CONSTITUIÇÃO_BRASILEIRA_DE_1988_1>.

MAIA, Lorena Duarte Lopes - **Colisão de direitos fundamentais: visão do Supremo Tribunal Federal** [Em linha], atual. 2012. [Consult. 22 jul. 2019]. Disponível em WWW:<URL:https://ambitojuridico.com.br/cadernos/direito-constitucional/colisao-de-direitos-fundamentais-visao-do-supremo-tribunal-federal/>.

MINNAAR, Anthony - **The implementation and impact of crime prevention/crime control open street Closed-Circuit Television surveillance in South African Central Business Districts** [Em linha], atual. 2007. [Consult. 6 mar. 2019]. Disponível em WWW:<URL:https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3447/3410>.

MINUSCOLI, Alcenir Luis; ALMEIDA, Luis Henrique Fogaça De - **Afinal o que é segurança pública?** [Em linha], atual. 2016. [Consult. 2 jan. 2019]. Disponível em WWW:<URL:https://jus.com.br/artigos/51752/afinal-o-que-e-seguranca-publica>.

MONTESQUIEU, Charles - **O Espírito das Leis**. São Paulo : Martins Fontes, 2000

MORAES, Alexandre De - **Direitos humanos fundamentais: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência**. São Paulo : Atlas, 2003

MORAES, Alexandre De - **Direito Constitucional**. São Paulo : Atlas, 2006

MPDFT - **Participe da audiência pública que vai debater o uso de tecnologias de reconhecimento facial - MPDFT** [Em linha], atual. 2019. [Consult. 8 jul. 2019]. Disponível em WWW:<URL:http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10769-participe-da-audiencia-publica-que-vai-debater-uso-de-tecnologias-de-reconhecimento-facial>.

MÜLLER, Christoph; BOOS, Daniel - **Zurich Main Railway Station: A Typology of Public CCTV Systems** [Em linha], atual. 2004. [Consult. 20 fev. 2019]. Disponível em WWW:<URL:https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3372/3335>.

NÓBREGA MALDONADO, Viviane; OPICE BLUM, Renato - **Comentários ao RGPD – Regulamento Geral sobre a Proteção de Dados da União Europeia**. São Paulo : Thomson Reuters Brasil, 2018

NORRIS, Clive; MCCAHILL, Mike; WOOD, David - **The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space** [Em linha], atual. 2004. [Consult. 15 fev. 2019]. Disponível em WWW:<URL:https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3369/3332>.

OBSERVADOR - **Na China, há polícias a usar óculos com reconhecimento facial para identificar cidadãos** [Em linha], atual. 2018. [Consult. 25 mar. 2019]. Disponível em WWW:<URL:https://observador.pt/2018/02/08/na-china-ha-policias-a-usar-oculos-com-reconhecimento-facial-para-identificar-cidadaos>.

ORWELL, George - **1984**. Lisboa : Antígona, 2007

PEREIRA, Marcelo Cardoso - **Direito à intimidade**. Curutiba : Juruá, 2003

PINHEIRO, Patrícia Peck - **Proteção de Dados Pessoais – Comentários à Lei n. 13.709/2018 (LGPD) da autora . (Locais do Kindle 191-194). . Edição**. São Paulo : Saraiva Educação, 2018

PIZA, Eric L. *et al.* - **CCTV and Crime Prevention - A new Systematic Review and Meta-Analysis**. Estocolmo : Swedish National Council for Crime Prevention, 2018

REBELLO, Aiuri - **Bancada do PSL vai à China conhecer sistema que reconhece rosto de cidadãos** [Em linha], atual. 2019. [Consult. 25 mar. 2019]. Disponível em WWW:<URL:https://www1.folha.uol.com.br/mercado/2019/01/bancada-do-psl-vai-a-china-importar-sistema-que-reconhece-rosto-de-cidadaos.shtml>.

REDAÇÃO CORREIO - **Salvador registra primeira prisão por reconhecimento facial** [Em linha], atual. 2019. [Consult. 27 mar. 2019]. Disponível em WWW:<URL:https://www.correio24horas.com.br/noticia/nid/salvador-registra-primeira-prisao-por-reconhecimento-facial/>.

ROUSSEAU, Jean-Jacques - **O Contrato Social**. São Paulo : Martins Fontes, 1999

SAMPAIO, José Adércio Leite - **Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte**. Belo Horizonte : Del Rey, 1998

SECRETARIA-GERAL DA PRESIDÊNCIA DO BRASIL - **Custos econômicos da criminalidade no Brasil** [Em linha] Disponível em WWW:<URL:https://cidades.ibge.gov.br/brasil/ba/panorama>.

SILVA, Edson Ferreira Da - **Direito à intimidade: de acordo com a doutrina, o direito comparado, a Constituição de 1988 e o Código Civil de 2002**. São Paulo : Juarez Soares, 2003

SILVA NETO, Amaro Moraes E - **Privacidade na internet: um enfoque jurídico**. Bauru : Edipro, 2001

SOUTH WALES POLICE - **Smarter Recognition Safer Community - South Wales Police** [Em linha], atual. 2019. [Consult. 20 mar. 2019]. Disponível em WWW:<URL:http://afr.south-wales.police.uk/smarter-recognition>.

TEICHER, Jordan G. - **Gazing Back at the Surveillance Cameras That Watch Us - The New York Times** [Em linha], atual. 2018. [Consult. 13 mar. 2019]. Disponível em WWW:<URL:https://www.nytimes.com/2018/08/13/lens/surveillance-camera-photography.html>.

UNITED NATIONS OFFICE ON DRUGS AND CRIME - **Intentional Homicide Victims** [Em linha], atual. 2018. [Consult. 1 fev. 2019]. Disponível em WWW:<URL:https://dataunodc.un.org/crime/intentional-homicide-victims>.

VIEIRA, Oscar Vlhena - **Direitos fundamentais: uma leitura da jurisprudência do STF**. São Paulo : Malheiros, 2006

VIEIRA, Tatiana Malta - **O direito à privacidade na sociedade da informação: efetivação desse direito fundamental diante dos avanços da tecnologia da informação**. Porto Alegre : Fabris, 2007

WALTON, Greg - **China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China**. [S.l.] : International Centre for Human Rights and Democratic Development, 2001, atual. 2001.

WEBER, Max - **Ciência e Política: Duas vocações**. São Paulo : Martin Claret, 2015

WOLFORD, Ben - **What is the GDPR, the EU's new data protection law?** [Em linha],

atual. 2019. [Consult. 8 jul. 2019]. Disponível em WWW:<URL:https://gdpr.eu/what-is-gdpr/>.

WORLD HEALTH ORGANIZATION - **World health statistics 2018: monitoring health for the SDGs, sustainable development goals**. Genebra : World Health Organization, 2018

XINHUA - **Facial recognition technology helps Chinese police solve crimes** [Em linha], atual. 2018. [Consult. 25 mar. 2019]. Disponível em WWW:<URL:http://www.chinadaily.com.cn/a/201804/11/WS5acdd4bda3105cdcf6517a46.html>.

YOUTUBE - **Youtube - Audiência Pública - Reconhecimento Facial** [Em linha], atual. 2019. [Consult. 8 jul. 2019]. Disponível em WWW:<URL:https://www.youtube.com/watch?v=pmzvXcevJr4>.